PURE AND APPLIED MATHEMATICS
A SERIES OF MONOGRAPHS AND TEXTBOOKS

Quadratic Irrationals

An Introduction to Classical Number Theory

Franz Halter-Koch

CRC Press
Taylor & Francis Group
A CHAPMAN & HALL BOOK

Quadratic Irrationals

An Introduction to
Classical Number Theory

PURE AND APPLIED MATHEMATICS

A Program of Monographs, Textbooks, and Lecture Notes

EXECUTIVE EDITORS

Earl J. Taft
Rutgers University
Piscataway, New Jersey

Zuhair Nashed
University of Central Florida
Orlando, Florida

EDITORIAL BOARD

Jane Cronin
Rutgers University

S. Kobayashi
University of California, Berkeley

Marvin Marcus
University of California, Santa Barbara

W. S. Massey
Yale University

Anil Nerode
Cornell University

Freddy van Oystaeyen
University of Antwerp, Belgium

Donald Passman
University of Wisconsin, Madison

Fred S. Roberts
Rutgers University

David L. Russell
Virginia Polytechnic Institute and State University

Walter Schempp
Universität Siegen

MONOGRAPHS AND TEXTBOOKS IN PURE AND APPLIED MATHEMATICS

Recent Titles

Kevin J. Hastings, Introduction to the Mathematics of Operations Research with *Mathematica*®, Second Edition (2006)

Robert Carlson, A Concrete Introduction to Real Analysis (2006)

John Dauns and Yiqiang Zhou, Classes of Modules (2006)

N. K. Govil, H. N. Mhaskar, Ram N. Mohapatra, Zuhair Nashed, and J. Szabados, Frontiers in Interpolation and Approximation (2006)

Luca Lorenzi and Marcello Bertoldi, Analytical Methods for Markov Semigroups (2006)

M. A. Al-Gwaiz and S. A. Elsanousi, Elements of Real Analysis (2006)

Theodore G. Faticoni, Direct Sum Decompositions of Torsion-Free Finite Rank Groups (2007)

R. Sivaramakrishnan, Certain Number-Theoretic Episodes in Algebra (2006)

Aderemi Kuku, Representation Theory and Higher Algebraic K-Theory (2006)

Robert Piziak and P. L. Odell, Matrix Theory: From Generalized Inverses to Jordan Form (2007)

Norman L. Johnson, Vikram Jha, and Mauro Biliotti, Handbook of Finite Translation Planes (2007)

Lieven Le Bruyn, Noncommutative Geometry and Cayley-smooth Orders (2008)

Fritz Schwarz, Algorithmic Lie Theory for Solving Ordinary Differential Equations (2008)

Jane Cronin, Ordinary Differential Equations: Introduction and Qualitative Theory, Third Edition (2008)

Su Gao, Invariant Descriptive Set Theory (2009)

Christopher Apelian and Steve Surace, Real and Complex Analysis (2010)

Norman L. Johnson, Combinatorics of Spreads and Parallelisms (2010)

Lawrence Narici and Edward Beckenstein, Topological Vector Spaces, Second Edition (2010)

Moshe Sniedovich, Dynamic Programming: Foundations and Principles, Second Edition (2010)

Drumi D. Bainov and Snezhana G. Hristova, Differential Equations with Maxima (2011)

Willi Freeden, Metaharmonic Lattice Point Theory (2011)

Murray R. Bremner, Lattice Basis Reduction: An Introduction to the LLL Algorithm and Its Applications (2011)

Clifford Bergman, Universal Algebra: Fundamentals and Selected Topics (2011)

A. A. Martynyuk and Yu. A. Martynyuk-Chernienko, Uncertain Dynamical Systems: Stability and Motion Control (2012)

Washek F. Pfeffer, The Divergence Theorem and Sets of Finite Perimeter (2012)

Willi Freeden and Christian Gerhards, Geomathematically Oriented Potential Theory (2013)

Anatoly Martynyuk, Larisa Chernetskaya, and Vladislav Martynyuk, Weakly Connected Nonlinear Systems: Boundedness and Stability of Motion (2013)

Franz Halter-Koch, Quadratic Irrationals: An Introduction to Classical Number Theory (2013)

This page intentionally left blank

Quadratic Irrationals

An Introduction to Classical Number Theory

Franz Halter-Koch
University of Graz
Austria

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
A CHAPMAN & HALL BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

© 2013 by Taylor & Francis Group, LLC
CRC Press is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works
Version Date: 20130422

International Standard Book Number-13: 978-1-4665-9184-4 (eBook - General)

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, please access www.copyright.com (http://www.copyright.com/) or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. CCC is a not-for-profit organization that provides licenses and registration for a variety of users. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged.

Trademark Notice: Product or corporate names may be trademarks or registered trademarks, and are used only for identification and explanation without intent to infringe.

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the CRC Press Web site at
http://www.crcpress.com

Für Dörthi

This page intentionally left blank

Foreword

The central subject of this volume is the number theory of quadratic irrationals in its various manifestations : Continued fractions, orders in quadratic number fields, and binary quadratic forms. These are the classical objects studied by the famous number theorists of the 18th and 19th century, above all Gauss, Legendre, Lagrange and Dirichlet. Until today this subject has continued to be an attractive topic of research producing a wealth of interesting and beautiful results. However, the literature on the subject is scattered, the notation is far from being standardized, and an interested reader will hardly find a unifying approach for the different aspects of the subject. Of course, basic results of the theory can be found in almost every textbook on (elementary) number theory. Among the books, which present parts of the classical theory in a more comprehensive way, I should mention the beautiful old book of L. E. Dickson [**21**], O. Perron's classical book on continued fractions [**90**], D. Flath's book [**27**] for an up-to-date and thorough presentation of Gauss' theory of binary quadratic forms, R. Mollin's book [**74**] for the arithmetic of quadratic orders and their computational aspects, and D. A. Buell's book [**13**] on computations in connection with quadratic forms. An important source for the classical theory of binary quadratic forms is the set of lecture notes by P. Kaplan [**51**]. It is very unfortunate that they have never been made accessible for a wider audience. A more popular but recommendable overview of the theory of binary quadratic forms discussing the development of the theory from Gauss to date is Chapter 6 in P. Ribenboim's book [**92**].

There is an important connection between the elementary theory of quadratic irrationals and higher algebraic number theory which is not addressed in the above-mentioned books and will also not be the subject of the present volume. These aspects are dealt with in several textbooks of algebraic number theory. For a further reading in this direction the reader is referred to the books of H. Cohn [**18**] (addressing the connection with ring class fields), D. Cox [**19**] (addressing the connection with complex multiplication), and F. Lemmermeyer [**67**] (addressing the connection with reciprocity laws). The reader is also invited to consult Chapter 9 in H. Koch's book [**62**] and the survey articles by W. Narkiewicz [**82**] and J. Oesterle [**86**].

The present volume arose from a series of lectures on quadratic irrationals which I gave for students with modest backgrounds in elementary algebra and number theory, dealing with continued fractions, binary quadratic forms, class groups and the arithmetic of quadratic orders in a consistent way.

It is the objective of this book to present the classical theory of continued fractions, quadratic orders, binary quadratic forms and class groups in a unified way based on the concept of a quadratic irrational. Aside from the most classical topics, the reader will find several beautiful and important recent results which, up to now, are scattered in the literature and difficult to access. Among them I would like to mention special results on binary quadratic Diophantine equations and continued fractions, explicit biquadratic class group characters, the divisibility of class numbers by 16, F. Mertens' proof of Gauss' duplication theorem and a theory of binary quadratic forms which, in almost all places, departs from the restriction to fundamental discriminants. In two chapters, (modest) analytic tools are used: In Chapter 4 to prove Dirichlet's theorem on primes in arithmetic progressions, and in Chapter 8 to present Dirichlet's class number formula and to show that every primitive binary quadratic form represents infinitely many primes.

I am indebted to an anonymous referee for valuable hints and suggestions, and I want to thank my partners at Taylor & Francis for the fruitful and complaisant cooperation.

Introduction and Preface to the Reader

The reader is assumed to have some basic knowledge of elementary algebra, number theory and analysis. In Appendix A, we have collocated the basics from elementary algebra and number theory in a concise way (partly with detailed proofs). For a thorough introduction to elementary algebra and number theory, the reader is referred to any introductory book on algebra or elementary number theory. Although voluminous, S. Lang's book [**64**] is a good source for all these things, but also a more modest introduction into elementary algebra will do the job.

An algebraically unexperienced reader might use Appendix A to update his algebraic fundamentals. Besides the basics, Appendix A contains some maybe less known special results, but there are precise references in the main text when they are used. Modest analytic methods are used in Chapter 4 and in Chapter 8. Appendix B contains some facts from real and complex analysis which are usually not covered in basic courses.

Although the content of the various chapters can be seen from their headings, I will briefly describe the main features of each chapter and their interconnections. Adequate cross references make it possible to read (at least partially) the various chapters independently.

Chapter 1 contains the basic notions of quadratic irrationals and their equivalence via the modular group. The concepts and notations introduced there are essential for the whole volume. The finiteness of the class number for real quadratic irrationals however will only be proved in Chapter 2 when the theory of continued fractions is at our disposal.

In Chapter 2, we present the classical theory of simple continued fractions with an emphasis on real quadratic irrationals. In particular, the reader will find here an extensive theory of Pell's equation and the continued fraction expansion of special quadratic irrationals. The reduction theory of indefinite binary quadratic forms (in Chapter 6) and the structure of cycles of regular ideals in quadratic orders (in Chapter 5) will be based on these results.

Chapter 3 is addressed to the classical quadratic reciprocity law. We introduce Gauss and Jacobi sums in order to give short and concise proofs of the quadratic reciprocity law and Fermat's two squares theorem. The theory of Gauss and Jacobi sums is used again in Chapter 4 for the summation of Dirichlet's L-series and, more intensively, in Chapter 7 for the investigation of cubic and biquadratic reciprocity. The final section of Chapter 3 deals with the structure of quadratic characters in general (this is used in Chapter 6 for the presentation of Gauss' genus theory).

Chapter 4 contains a self-contained proof of Dirichlet's theorem on primes in arithmetic progressions, based on the theory of Dirichlet's L-series. The necessary (modest) analytic tools are collocated in Appendix B. Analytic methods are used again only in Chapter 8. A reader who wants to skip analytic methods at a first reading can do this without any problems.

Chapter 5 is central. It contains the ideal theory of quadratic orders, based on the description of regular ideals by quadratic irrationals. We introduce class groups and class semigroups, describe explicitly the structure of ambiguous ideals and ideal classes and apply the results to the theory of Diophantine equations of Pellian type. Then we investigate prime decomposition and multiplicative ideal theory of quadratic orders and connect the class groups of distinct orders by means of the Mayer-Vietoris exact sequence. The chapter ends with an amusing connection between class numbers and Fibonacci numbers.

Chapter 6 is devoted to Gauss' theory of binary quadratic forms with an emphasis on the connection with quadratic irrationals and regular ideals in quadratic orders. Here the close connection between the various concepts of the theory becomes lucid. Although composition of quadratic forms is defined using ideal theory, most of the classical results (given in the language of forms) are proved. The presentation of genus theory is based on the theory of quadratic characters presented in Chapter 3. Three different proofs of Gauss' duplication theorem are given : Gauss' original proof using ternary forms, Dirichlet's proof using primes in arithmetic progression, and Mertens' elementary (but artificial) proof which runs completely inside the theory of binary forms. The chapter closes with a section containing the classical results on the representation of positive integers as sums of squares.

Chapter 7 deals with cubic and biquadratic reciprocity. The reciprocity laws are proved in the corresponding domains of roots of unity and followed by a detailed discussion of cubic and biquadratic power residue criteria and rational biquadratic laws. Several of these results have an elegant interpretation and a simple proof in the context of higher algebraic number theory (for this the interested reader should consult [**67**]). Here we intentionally content ourselves to the elementary approach (however with several new proofs). The section ends with Z.-H. Sun's construction of a biquadratic class group character and its applications.

In Chapter 8 analytic methods are used again. First, the analytic class number formula for quadratic orders is proved and some of its classical consequences are discussed. After that, we introduce L-series of quadratic orders and prove that every primitive binary form represents infinitely many primes. All this is done for arbitrary (and not necessarily fundamental) quadratic discriminants. Two final sections are addressed to the structure of 2-class groups, in particular in the cyclic case. Criteria for cyclic 2-class groups to have an order divisible by 8 and 16 are given, and connections with biquadratic residues are dealt with.

Several exercises are sprinkled throughout the volume. Most of them are elementary, and references are given for some more involved ones. An ambitious reader who wants to do more is referred to the voluminous exercise sections in the books of D. A. Cox [**19**], D. E. Flath [**27**] and F. Lemmermeyer [**67**]. I could just as well have copied them into the present volume.

Notations

For sets A, B, we write $A \subsetneq B$ or $B \supsetneq A$ if A is a proper subset of B. The notions $A \subset B$ and $B \supset A$ include the case $A = B$.

We denote by

- $\mathbb{N}_0$ the set of non-negative integers;
- $\mathbb{N} = \mathbb{N}_0 \setminus \{0\}$ the set of positive integers;
- $\mathbb{P}$ the set of prime numbers;
- $\mathbb{Z}$ the ring of integers, and $\mathbb{Q}$ the field of rational numbers;
- $\mathbb{R}$ the field of real numbers, and $\mathbb{C}$ the field of complex numbers;
- $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ the field of p elements for a prime p;
- $|A| \in \mathbb{N}_0 \cup \{\infty\}$ the number of elements of a set A;
- $A^\bullet$ the set of non-zero elements of a set A.

We use the self-explaining notations $\mathbb{R}_{>0}$, $\mathbb{R}_{\ge 0}$, $\mathbb{Q}_{>0}$, $\mathbb{N}_{\ge 2}$ etc. For a, $b \in \mathbb{Z}$, we set $[a, b] = \{x \in \mathbb{Z} \mid a \le x \le b\}$ if there is no danger of confusion with the real interval, and we set $[a, b] = \emptyset$ if $a > b$.

For a real number x, we set

$$\lfloor x \rfloor = \max\{g \in \mathbb{Z} \mid g \le x\}\,, \qquad \lceil x \rceil = \min\{g \in \mathbb{Z} \mid g \ge x\}\,,$$

and we denote by $\operatorname{sgn}(x) \in \{0, \pm 1\}$ its sign. For a complex number z, we denote by $\Re(z)$ its real part and by $\Im(z)$ its imaginary part. We normalize $\sqrt{z}$ by $\sqrt{z} \ge 0$ if $z \in \mathbb{R}_{\ge 0}$, and $\Im(\sqrt{z}\,) \ge 0$ if $z \in \mathbb{C} \setminus \mathbb{R}_{\ge 0}$.

Euler's constant is denoted by e, and the imaginary unit is denoted by i. For $\vartheta \in \mathbb{R}$, we denote the open and the closed right half-plane determined by ϑ by

$$\mathcal{H}_\vartheta = \{s \in \mathbb{C} \mid \Re(s) > \vartheta\} \quad \text{and} \quad \overline{\mathcal{H}}_\vartheta = \{s \in \mathbb{C} \mid \Re(s) \ge \vartheta\}\,.$$

For x, $X \in \mathbb{R}$ and $m \in \mathbb{N}$, we write

$$\sum_{n<x}, \quad \sum_{x \le n < X}, \quad \sum_{n>X}, \quad \sum_{n \,|\, m} \quad \text{etc.} \quad \text{resp.} \quad \sum_{p<x}, \quad \sum_{x \le p < X}, \quad \sum_{p>X}, \quad \sum_{p \,|\, m} \quad \text{etc.}$$

to denote the (eventually infinite) sum over all $n \in \mathbb{N}$ respectively all primes p satisfying the corresponding conditions.

With a few exceptions, all groups considered in this volume are abelian and the composition is written either additively or multiplicatively. If G is a group, $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in G$, then we denote by

- $[a_1, \ldots, a_n] = \mathbb{Z}a_1 + \ldots + \mathbb{Z}a_n = \{k_1a_1 + \ldots + k_na_n \mid k_1, \ldots, k_n \in \mathbb{Z}\}$ the subgroup of G generated by $a_1, \ldots, a_n$ if G is an additive group (although we will use brackets also to denote simple continued fractions and binary quadratic forms, there will be no danger of confusion);
- $\langle a_1, \ldots, a_n \rangle = \{a_1^{k_1} \cdot \ldots \cdot a_n^{k_n} \mid k_1, \ldots, k_n \in \mathbb{Z}\}$ the subgroup of G generated by $a_1, \ldots, a_n$ if G is a multiplicative group.

By a ring R we always mean an associative and commutative ring with a unit element $1 \in R$.

This page intentionally left blank

Contents

Foreword ix

Introduction and Preface to the Reader xi

Notations xiii

Chapter 1. Quadratic irrationals 1
- 1.1. Quadratic irrationals, quadratic number fields and discriminants 1
- 1.2. The modular group 7
- 1.3. Reduced quadratic irrationals 16
- 1.4. Two short tables of class numbers 21

Chapter 2. Continued fractions 25
- 2.1. General theory of continued fractions 25
- 2.2. Continued fractions of quadratic irrationals I: General theory 38
- 2.3. Continued fractions of quadratic irrationals II: Special types 50

Chapter 3. Quadratic residues and Gauss sums 63
- 3.1. Elementary theory of power residues 63
- 3.2. Gauss and Jacobi sums 67
- 3.3. The quadratic reciprocity law 72
- 3.4. Sums of two squares 79
- 3.5. Kronecker and quadratic symbols 82

Chapter 4. L-series and Dirichlet's prime number theorem 99
- 4.1. Preliminaries and some elementary cases 99
- 4.2. Multiplicative functions 102
- 4.3. Dirichlet L-functions and proof of Dirichlet's theorem 106
- 4.4. Summation of L-series 112

Chapter 5. Quadratic orders 115
- 5.1. Lattices and orders in quadratic number fields 115
- 5.2. Units in quadratic orders 121
- 5.3. Lattices and (invertible) fractional ideals in quadratic orders 129
- 5.4. Structure of ideals in quadratic orders 132
- 5.5. Class groups and class semigroups 140
- 5.6. Ambiguous ideals and ideal classes 147
- 5.7. An application: Some binary Diophantine equations 160
- 5.8. Prime ideals and multiplicative ideal theory 174
- 5.9. Class groups of quadratic orders 179

Chapter 6. Binary quadratic forms 191
6.1. Elementary definitions and equivalence relations 191
6.2. Representation of integers 199
6.3. Reduction 210
6.4. Composition 213
6.5. Theory of genera 221
6.6. Ternary quadratic forms 240
6.7. Sums of squares 248

Chapter 7. Cubic and biquadratic residues 257
7.1. The cubic Jacobi symbol 257
7.2. The cubic reciprocity law 263
7.3. The biquadratic Jacobi symbol 271
7.4. The biquadratic reciprocity law 279
7.5. Rational biquadratic reciprocity laws 289
7.6. A biquadratic class group character and applications 306

Chapter 8. Class groups 321
8.1. The analytic class number formula 322
8.2. L-functions of quadratic orders 332
8.3. Ambiguous classes and classes of order divisibility by 4 340
8.4. Discriminants with cyclic 2-class group: Divisibility by 8 and 16 345

Appendix A. Review of elementary algebra and number theory 359
A.1. Fundamentals of group theory 359
A.2. Fundamentals of ring theory 362
A.3. Elementary arithmetic in $\mathbb{Z}$ 365
A.4. Lattices 372
A.5. Finite abelian groups 375
A.6. Prime residue class groups 380
A.7. Roots of unity and characters of finite abelian groups 384
A.8. Factorization in integral domains 389
A.9. Algebraic integers 394

Appendix B. Some results from analysis 399
B.1. Notational conventions and results from complex analysis 399
B.2. Further analytic tools 401

Bibliography 407

List of Symbols 411

Subject Index 413

CHAPTER 1

Quadratic irrationals

Quadratic irrationals are the non-rational roots of quadratic equations with rational coefficients. Integral binary quadratic forms, binary Diophantine equations and the theory of quadratic orders are central objects of classical number theory controlled by quadratic irrationals. In this volume, we consider quadratic irrationals as the central notion and rely on them in the other topics of the theory.

In the context of binary quadratic forms, the theory goes back to C. F. Gauss [**32**] and P. G. L. Dirichlet [**23**]. For the approach chosen here, we refer to the book [**70**] and the articles [**58**], [**40**], [**4**] and [**113**].

1.1. Quadratic irrationals, quadratic number fields and discriminants

For a complex number z we normalize its square root $\sqrt{z}$ such that $\sqrt{z} \ge 0$ if $z \in \mathbb{R}_{\ge 0}$, and $\Im(\sqrt{z}) \ge 0$ otherwise. Then it follows that $\sqrt{q^2 z} = |q|\sqrt{z}$ for all $z \in \mathbb{C}$ and $q \in \mathbb{R}$.

A *quadratic irrational* is a complex number $\xi \in \mathbb{C} \setminus \mathbb{Q}$ which satisfies an equation $\xi^2 + p\xi + q = 0$ for some $p,\ q \in \mathbb{Q}$. If ξ satisfies such an equation, then

$$\xi = -\frac{p}{2} + \varepsilon\sqrt{\frac{p^2}{4} - q} \quad \text{for some } \varepsilon \in \{\pm 1\}\,, \quad \text{and} \quad \frac{p^2}{4} - q \in \mathbb{Q} \quad \text{is not a square.}$$

Note that ε, p and q are uniquely determined by ξ. Indeed, the uniqueness of ε follows from the normalization of the square root, and if $\xi^2 + p_1\xi + q_1 = 0$ for some $p_1,\ q_1 \in \mathbb{Q}$, then $(p - p_1)\xi = q_1 - q$, and as $\xi \notin \mathbb{Q}$, we get $p = p_1$ and $q = q_1$. The polynomial

$$X^2 + pX + q \in \mathbb{Q}[X]$$

is called the *minimal polynomial* of ξ. It has a factorization

$$X^2 + pX + q = (X - \xi)(X - \xi')\,, \quad \text{where} \quad \xi' = -\frac{p}{2} - \varepsilon\sqrt{\frac{p^2}{4} - q},.$$

The complex number ξ' is called the *conjugate*, $\mathcal{T}(\xi) = -p$ is called the *trace*, $\mathcal{N}(\xi) = q$ is called the *norm* and ε is called the *signature* of ξ. By definition, ξ and ξ' have the same minimal polynomial (hence the same trace and the same norm), but distinct signatures, and $\xi'' = \xi$. Two quadratic irrationals coincide if and only if they have the same norm, the same trace and the same signature.

For $b \in \mathbb{Q}$, we set $b' = b$, $\mathcal{T}(b) = 2b$ and $\mathcal{N}(b) = b^2$. Then it follows that $\mathcal{T}(x) = x + x'$ and $\mathcal{N}(x) = xx'$ whenever x is either a quadratic irrational or a rational number.

A quadratic irrational ξ is called *real* if $\xi \in \mathbb{R}$, and *complex* otherwise. If ξ is a complex quadratic irrational, then $\xi' = \overline{\xi}$, $\mathcal{T}(\xi) = 2\Re(\xi)$ and $\mathcal{N}(\xi) = |\xi|^2$.

A complex number ξ is a quadratic irrational if and only if

$$\xi = u + v\sqrt{d} \quad \text{for some } u,\, v,\, d \in \mathbb{Q} \quad \text{such that} \quad v \neq 0 \text{ and } d \text{ is not a square.}$$

If ξ is as above, then $\xi = u + \operatorname{sgn}(v)\sqrt{v^2 d}$, and $X^2 - 2uX + (u^2 - v^2 d)$ is the minimal polynomial of ξ. It follows that $\xi' = u - v\sqrt{d}$, $\mathcal{T}(\xi) = 2u$, $\mathcal{N}(\xi) = u^2 - v^2 d$ and $\operatorname{sgn}(v)$ is the signature of ξ. In particular, u and $\operatorname{sgn}(v)$ are uniquely determined by ξ. The following lemma is addressed to the uniqueness of v and d.

Lemma 1.1.1. *Every quadratic irrational ξ has a unique representation in the form $\xi = u + v\sqrt{d}$, where $u,\, v \in \mathbb{Q}$, $v \neq 0$ and $d \in \mathbb{Z} \setminus \{1\}$ is squarefree.*

PROOF. *Existence*: Let ξ be a quadratic irrational, say $\xi = u + v_1\sqrt{d_1}$, where $u,\, v_1,\, d_1 \in \mathbb{Q}$, $v_1 \neq 0$ and d_1 is not a square. By Theorem A.3.3, $d_1 = dq^2$, where $d \in \mathbb{Z}$ is squarefree and $q \in \mathbb{Q}_{>0}$. It follows that $d \neq 1$, and $\xi = u + qv_1\sqrt{d}$.

Uniqueness: Suppose that $\xi = u + v\sqrt{d} = u_1 + v_1\sqrt{d_1}$, where $u,\, u_1,\, v,\, v_1 \in \mathbb{Q}$, $vv_1 \neq 0$, and $d,\, d_1 \in \mathbb{Z} \setminus \{1\}$ are squarefree. Then we have already seen above that $u = u_1 = \mathcal{T}(\xi)/2$, and $\operatorname{sgn}(v) = \operatorname{sgn}(v_1)$ is the signature of ξ. It follows that $v^2 d = v_1^2 d_1$, hence $d = d_1$ and $|v| = |v_1|$ by the uniqueness in Theorem A.3.3, and $v = v_1$, since $\operatorname{sgn}(v) = \operatorname{sgn}(v_1)$. □

If ξ is a quadratic irrational, then the unique squarefree integer $d \in \mathbb{Z} \setminus \{1\}$ such that $\xi = u + v\sqrt{d}$ for some $u,\, v \in \mathbb{Q}$ is called the *radicand* of ξ. If $a \in \mathbb{Z}$ is not a square, then the radicand of $\sqrt{a}$ is just the squarefree kernel of a.

Although the radicand of a quadratic irrational is an obvious invariant, it is not the most important one. In the following Theorem 1.1.2 we will define the type and the discriminant of a quadratic irrational, and in the sequel we will see that these quantities are the invariants which are responsible for its deeper arithmetical properties.

Theorem and Definition 1.1.2. *Let ξ be a quadratic irrational.*

1. *There exists a unique triple $(a,b,c) \in \mathbb{Z}^3$ such that $(a,\, b,\, c) = 1$, $a \neq 0$, $b^2 - 4ac$ is not a square, and*

$$\xi = \frac{b + \sqrt{b^2 - 4ac}}{2a}\,.$$

   If this is the case, then $a\xi^2 - b\xi + c = 0$, $\mathcal{T}(\xi) = a^{-1}b$, $\mathcal{N}(\xi) = a^{-1}c$, and $\operatorname{sgn}(a)$ is the signature of ξ.

   We call (a,b,c) the *type* and $\Delta = b^2 - 4ac$ the *discriminant* of ξ. By definition, ξ is real if $\Delta > 0$, and imaginary if $\Delta < 0$.

2. *Let ξ be of type (a,b,c) and $(a_1,b_1,c_1) \in \mathbb{Z}^3$ such that $a_1\xi^2 + b_1\xi + c_1 = 0$. Then there exists some $y \in \mathbb{Z}$ such that $a_1 = ay$, $b_1 = -by$ and $c_1 = cy$.*
3. *Let Δ be the discriminant of ξ, and let $a_1,\, b_1 \in \mathbb{Z}$ be such that $a_1 \neq 0$ and*

$$\xi = \frac{b_1 + \sqrt{\Delta}}{2a_1}\,.$$

Then $\Delta = b_1^2 - 4a_1c_1$ *for some* $c_1 \in \mathbb{Z}$*, and* ξ *is of type* (a_1, b_1, c_1)*.*

Proof. 1. Assume that $\xi = u + v\sqrt{d}$, where $u,\ v,\ d \in \mathbb{Q}$, $\ v \neq 0$ and d is not a square. By Theorem A.3.2, there exist uniquely determined integers $a,\ b,\ c \in \mathbb{Z}$ such that

$$a \neq 0\,, \quad \operatorname{sgn}(a) = \operatorname{sgn}(v)\,, \quad 2u = \frac{b}{a}\,, \quad u^2 - v^2 d = \frac{c}{a} \quad \text{and} \quad (a,b,c) = 1\,.$$

Then $b^2 - 4ac = 4a^2v^2d$ is not a square,

$$v^2 d = u^2 - \frac{c}{a} = \frac{b^2 - 4ac}{4a^2} \quad \text{and} \quad u + v\sqrt{d} = \frac{b + \sqrt{b^2 - 4ac}}{2a}\,.$$

To prove uniqueness, assume that $a,\ b,\ c \in \mathbb{Z}$, $\ (a,b,c) = 1$, $\ b^2 - 4ac$ is not a square (hence $a \neq 0$), and

$$\xi = \frac{b + \sqrt{b^2 - 4ac}}{2a}\,.$$

Then $\operatorname{sgn}(a)$ is the signature of ξ, $\ \mathcal{T}(\xi) = a^{-1}b$ and $\mathcal{N}(\xi) = a^{-1}c$. Hence the uniqueness of (a,b,c) follows by Theorem A.3.2.

2. If $a_1 = 0$, then $b_1 = c_1 = 0$ by the linear independence of $(1, \xi)$, and we set $y = 0$. Thus assume that $a_1 \neq 0$, and set $g = (a_1, b_1, c_1)$. There exists some $\varepsilon \in \{\pm 1\}$ such that

$$\xi = \frac{-b_1 + \varepsilon\sqrt{b_1^2 - 4a_1c_1}}{2a_1}\,,$$

and we set $a_2 = \varepsilon g^{-1}a_1$, $\ b_2 = -\varepsilon g^{-1}b_1$ and $c_2 = \varepsilon g^{-1}c_1$. Then $(a_2, b_2, c_2) = 1$,

$$\xi = \frac{b_2 + \sqrt{b_2^2 - 4a_2c_2}}{2a_2}\,,$$

and from the uniqueness in 1. we obtain $(a_2, b_2, c_2) = (a, b, c) \in \mathbb{Z}^3$. Hence $a_1 = g\varepsilon a$, $b_1 = -g\varepsilon b$ and $c_1 = g\varepsilon c$.

3. Let ξ be of type (a, b, c). By assumption, $\operatorname{sgn}(a_1) = \operatorname{sgn}(a)$ is the signature of ξ, and $4a_1^2\xi^2 - 4a_1b_1\xi + b_1^2 - \Delta = 0$. By 2., there is some $y \in \mathbb{Z}$ such that $4a_1^2 = ay$, $4a_1b_1 = by$ and $b_1^2 - \Delta = cy$. This implies

$$\Delta y^2 = (b^2 - 4ac)y^2 = 16a_1^2b_1^2 - 16a_1^2(b_1^2 - \Delta) = 16a_1^2\Delta\,,$$

hence $y = 4a_1\varepsilon$, where $\varepsilon \in \{\pm 1\}$, and therefore $4a_1^2 = ay = 4aa_1\varepsilon$. Consequently, we obtain $a_1 = a\varepsilon$, $\ \varepsilon = 1$, $\ b_1 = b$, and as $\Delta = b^2 - 4ac$, the assertion follows. $\square$

The roots of unity

$$\zeta_3 = \mathsf{e}^{2i\pi/3} = \frac{-1 + \mathsf{i}\sqrt{3}}{2}\,, \quad \zeta_4 = \mathsf{e}^{\mathsf{i}\pi/2} = \mathsf{i} \quad \text{and} \quad \zeta_6 = \mathsf{e}^{\mathsf{i}\pi/3} = \frac{1 + \mathsf{i}\sqrt{3}}{2}$$

are quadratic irrationals of types $(1, -1, 1)$, $\ (1, 0, 1)$ and $(1, 1, 1)$, and of discriminants -3, -4 and -3, respectively.

Exercise 1.1.3. Prove that the complex number

$$z = -\frac{3+2\mathrm{i}}{8+6\mathrm{i}}$$

is a quadratic irrational. Compute its type, its discriminant, its signature, its minimal polynomial, its trace and its norm.

Lemma 1.1.4. *Let* ξ *be a quadratic irrational of type* (a,b,c), $\Delta = b^2-4ac$ *its discriminant and* $n \in \mathbb{Z}$. *Then the numbers* $\xi+n$, $-\xi$, ξ', ξ^{-1}, $-\xi'$, ξ'^{-1}, $-\xi^{-1}$ *and* $-\xi'^{-1}$ *are also quadratic irrationals of discriminant* Δ, *namely*

$$\xi+n \ \text{ is of type } \ (a, b+2an, an^2+bn+c)\,, \quad -\xi \ \text{ is of type } \ (-a,b,-c)\,,$$

$$\xi' \ \text{ is of type } \ (-a,-b,-c)\,, \quad \xi^{-1} \ \text{ is of type } \ (-c,-b,-a)\,,$$

$$-\xi' \ \text{ is of type } \ (a,-b,c)\,, \quad \xi'^{-1} \ \text{ is of type } \ (c,b,a)\,,$$

$$-\xi^{-1} \ \text{ is of type } \ (c,-b,a) \quad \text{and} \quad -\xi'^{-1} \ \text{ is of type } \ (-c,b,-a)\,.$$

Exercise 1.1.5. Prove Lemma 1.1.4.

Next we study discriminants more closely for their own sake. We introduce quadratic number fields and fundamental discriminants as their fundamental invariants.

An integer $\Delta \in \mathbb{Z}$ is called a *quadratic discriminant* if Δ is not a square and $\Delta \equiv 0$ or $1 \bmod 4$. If ξ is a quadratic irrational of type (a,b,c) and discriminant $\Delta = b^2-4ac$, then Δ is a quadratic discriminant according to this definition.

For a quadratic discriminant Δ, we define

$$\omega_\Delta = \frac{\sigma_\Delta + \sqrt{\Delta}}{2}\,, \quad \text{where} \quad \sigma_\Delta = \begin{cases} 0 & \text{if} \quad \Delta \equiv 0 \mod 4\,, \\ 1 & \text{if} \quad \Delta \equiv 1 \mod 4\,. \end{cases}$$

If $\Delta = 4D+\sigma_\Delta$, where $D \in \mathbb{Z}$, then ω_Δ is a quadratic irrational of type $(1,\sigma_\Delta,-D)$ and discriminant Δ, $\omega_\Delta' = -\omega_\Delta+\sigma_\Delta$, and $\omega_\Delta^2 = D+\sigma_\Delta\omega_\Delta$. The quadratic irrational ω_Δ is called the *basis number* of discriminant Δ.

If Δ is a quadratic discriminant and $f \in \mathbb{N}$, then Δf^2 is also a quadratic discriminant (since $f^2 \equiv 0$ or $1 \bmod 4$). A quadratic discriminant Δ is called a *fundamental discriminant* if it is not of the form $\Delta = \Delta_1 f^2$ for some quadratic discriminant Δ_1 and an integer $f \geq 2$.

Theorem 1.1.6.

1. *For a quadratic discriminant* Δ, *the following assertions are equivalent*:
   (a) Δ *is a fundamental discriminant.*
   (b) *Either* Δ *is squarefree and* $\Delta \equiv 1 \bmod 4$, *or* $\Delta = 4D$ *for some squarefree integer* D *such that* $D \equiv 2$ *or* $3 \bmod 4$.
   (c) $\mathsf{v}_p(\Delta) \in \{0,1\}$ *for all odd primes* p, *and* $\Delta \equiv 1 \bmod 4$ *or* $\Delta \equiv 8 \bmod 16$ *or* $\Delta \equiv 12 \bmod 16$.

2. *Let $d \in \mathbb{Q}$ be not a square. Then there is a unique fundamental discriminant Δ_0 such that $d = \Delta_0 q^2$ for some $q \in \mathbb{Q}_{>0}$, and if d itself is a quadratic discriminant, then $q \in \mathbb{N}$.*
3. *Every quadratic irrational has a unique representation $\xi = u + v\sqrt{\Delta_0}$, where $u \in \mathbb{Q}$, $v \in \mathbb{Q}^\times$, and Δ_0 is a fundamental discriminant. In this case, there is some $f \in \mathbb{N}$ such that $\Delta_0 f^2$ is the discriminant of ξ.*

Proof. We apply Theorem A.3.3.

1. (a) $\Rightarrow$ (b) CASE 1: $\Delta \equiv 1 \bmod 4$. If Δ is not squarefree, then $\Delta = \Delta_1 f^2$ for some $\Delta_1 \in \mathbb{Z}$ and some odd integer $f \geq 2$. Then $\Delta_1 \equiv 1 \bmod 4$ is not a square and thus a quadratic discriminant, a contradiction.

CASE 2: $\Delta = 4D$ for some $D \in \mathbb{Z}$ which is not a square. If D is not squarefree, then $D = D_1 f^2$ for some $D_1 \in \mathbb{Z}$ and $f \geq 2$. But then $\Delta_1 = 4D_1$ is not a square, hence a quadratic discriminant, and $\Delta = \Delta_1 f^2$, a contradiction. If $D \equiv 1 \bmod 4$, then D is a quadratic discriminant and Δ is not a fundamental discriminant. Hence it follows that $D \equiv 2$ or $3 \bmod 4$, and $\Delta \equiv 8$ or $12 \bmod 16$.

(b) $\Rightarrow$ (c) $\Rightarrow$ (a) Obvious.

2. *Existence*: Suppose that $d = d_0 q_0^2$, where d_0 is the squarefree kernel of d and $q_0 \in \mathbb{Q}_{>0}$. If $d_0 \equiv 1 \bmod 4$, then d_0 is a fundamental discriminant, and we set $\Delta_0 = d_0$, $q = q_0$. If $d_0 \not\equiv 1 \bmod 4$, then $4d_0$ is a fundamental discriminant, and we set $\Delta_0 = 4d_0$, $q = q_0/2$. If d itself is a quadratic discriminant, then $q_0 \in \mathbb{Z}$, and if $d_0 \not\equiv 1 \bmod 4$, then $2 \mid q_0$. Hence we obtain $q \in \mathbb{Z}$ in either case.

Uniqueness: Suppose that $d = \Delta q^2 = \Delta_1 q_1^2$ with fundamental discriminants Δ, Δ_1 and q, $q_1 \in \mathbb{Q}_{>0}$. Then $\operatorname{sgn}(\Delta) = \operatorname{sgn}(\Delta_1)$ and $\mathsf{v}_p(\Delta) \equiv \mathsf{v}_p(\Delta_1) \bmod 2$ for all primes p. By 1. this is only possible if either $\Delta = \Delta_1$ or $\{\mathsf{v}_2(\Delta), \mathsf{v}_2(\Delta_1)\} = \{0, 2\}$, and we show that the latter case cannot occur. Indeed, assume the contrary, say $\mathsf{v}_2(\Delta) = 2$ and $\mathsf{v}_2(\Delta_1) = 0$. Then $\Delta = 4d$ and $d = \Delta_1 \equiv 1 \bmod 4$, a contradiction.

3. Let ξ be of type (a, b, c) and discriminant Δ.

Uniqueness: Let Δ_0 be a fundamental discriminant and $u \in \mathbb{Q}$, $v \in \mathbb{Q}^\times$ such that $\xi = u + v\sqrt{\Delta_0}$. Then $\xi^2 - 2u\xi + (u^2 - v^2\Delta_0) = 0$, and by the uniqueness of the minimal polynomial we obtain $2u = a^{-1}b$, $u^2 - v^2\Delta_0 = a^{-1}c$ and

$$\Delta = b^2 - 4ac = (2au)^2 - 4a^2(u^2 - v^2\Delta_0) = 4a^2v^2\Delta_0\,.$$

By 2., Δ_0 is uniquely determined by Δ, $f = |2av| \in \mathbb{N}$, and $\Delta = \Delta_0 f^2$. The uniqueness of u and v follows from the linear independence of $(1, \sqrt{\Delta_0}\,)$.

Existence: By 2., $\Delta = \Delta_0 f^2$, where $f \in \mathbb{N}$ and Δ_0 is a fundamental discriminant. Thus we obtain

$$\xi = \frac{b + \sqrt{\Delta}}{2a} = \frac{b}{2a} + \frac{f}{2a}\sqrt{\Delta_0}\,. \qquad \square$$

By Theorem 1.1.6.2, every quadratic discriminant Δ has a unique factorization $\Delta = \Delta_0 f_\Delta^2$, where Δ_0 is a fundamental discriminant and $f_\Delta \in \mathbb{N}$. We call Δ_0 the *fundamental discriminant associated with* Δ and f_Δ the *conductor* of Δ. In particular, Δ is a fundamental discriminant if and only if $f_\Delta = 1$. This terminology will be justified by the theory of quadratic orders in Chapter 5.

If ξ is a quadratic irrational, then the fundamental discriminant associated with its discriminant is called the *fundamental discriminant* of ξ.

An integer Δ is called a *prime discriminant* if either $\Delta = (-1)^{(p-1)/2}p$ for some odd prime p, or $\Delta \in \{-4, 8, -8\}$. By definition, a prime discriminant is a fundamental discriminant divisible by a single prime.

Exercise 1.1.7. Prove that every fundamental discriminant Δ has a unique factorization $\Delta = \Delta_1 \cdot \ldots \cdot \Delta_r$ into pairwise coprime fundamental discriminants $\Delta_1, \ldots, \Delta_r$, and that, conversely, any product of pairwise coprime prime discriminants is a fundamental discriminant.

For the quadratic discriminant $\Delta = -5280$, determine the associated fundamental discriminant Δ_0, the conductor, and write Δ_0 as a product of prime discriminants.

Definition 1.1.8. A *quadratic number field* K is a subfield of $\mathbb{C}$ satisfying $\dim_{\mathbb{Q}}(K) = 2$. It is called *real* if $K \subset \mathbb{R}$, and *imaginary* otherwise. For a quadratic irrational ξ, we define $\mathbb{Q}(\xi) = \mathbb{Q} + \mathbb{Q}\xi = \{x + y\xi \mid x, y \in \mathbb{Q}\} \subset \mathbb{C}$.

If ξ is a quadratic irrational and $\eta = a\xi + b$ for some $a, b \in \mathbb{Q}$ such that $a \neq 0$, then η is a quadratic irrational and $\mathbb{Q}(\xi) = \mathbb{Q}(\eta)$. In particular, if $z \in \mathbb{Q}(\xi) \setminus \mathbb{Q}$, then z is a quadratic irrational and $\mathbb{Q}(\xi) = \mathbb{Q}(z)$. If $\xi = u + v\sqrt{d}$, where $u, v, d \in \mathbb{Q}$, $v \neq 0$ and d is not a square, then $\mathbb{Q}(\xi) = \mathbb{Q}(\sqrt{d})$. If $u, u_1, v, v_1 \in \mathbb{Q}$, $\alpha = u + v\sqrt{d}$ and $\alpha_1 = u_1 + v_1\sqrt{d}$, then

$$\alpha \pm \alpha_1 = (u \pm u_1) + (v \pm v_1)\sqrt{d}\,, \quad \alpha\alpha_1 = (uu_1 + vv_1 d) + (uv_1 + u_1 v)\sqrt{d}\,,$$

and if $\alpha \neq 0$, then

$$\frac{1}{\alpha} = \frac{1}{u + v\sqrt{d}} = \frac{u}{u^2 - v^2 d} + \frac{-v}{u^2 - v^2 d}\sqrt{d}\,.$$

Therefore $\mathbb{Q}(\xi) = \mathbb{Q}(\sqrt{d})$ is a field, and it is in fact the smallest subfield of $\mathbb{C}$ containing ξ. If Δ is any quadratic discriminant and ξ is a quadratic irrational of discriminant Δ, then $\mathbb{Q}(\xi) = \mathbb{Q}(\sqrt{\Delta}\,)$.

Theorem and Definition 1.1.9. *Let K be a quadratic number field.*

1. *If $d, d_1 \in \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{d}\,) = \mathbb{Q}(\sqrt{d_1}\,)$, then $d_1 = db^2$ for some $b \in \mathbb{Q}$.*
2. *There exists a uniquely determined fundamental discriminant Δ_K such that $K = \mathbb{Q}(\sqrt{\Delta_K}\,)$, and then $K \setminus \mathbb{Q}$ is the set of all quadratic irrationals with fundamental discriminant Δ_K. In particular, if $K = \mathbb{Q}(\sqrt{\Delta}\,)$ for some quadratic discriminant Δ, then Δ_K is the fundamental discriminant associated with Δ.*

   Δ_K is called the *(field) discriminant* of K.
3. *The map $\iota\colon K \to K$, defined by $\iota(\alpha) = \alpha'$ for all $\alpha \in K$, is a field automorphism, and $\iota \,|\, \mathbb{Q} = \mathrm{id}_{\mathbb{Q}}$. In particular*

   $$\mathcal{N}(\alpha\beta) = \mathcal{N}(\alpha)\mathcal{N}(\beta) \ \text{ and } \ \mathcal{T}(\alpha + \beta) = \mathcal{T}(\alpha) + \mathcal{T}(\beta) \quad \text{for all } \alpha, \beta \in K\,.$$

Proof. 1. Let d, $d_1 \in \mathbb{Q}$ be such that $K = \mathbb{Q}(\sqrt{d}\,) = \mathbb{Q}(\sqrt{d_1}\,)$. Then we obtain $\sqrt{d_1} = a + b\sqrt{d}$ for some a, $b \in \mathbb{Q}$, and as $\sqrt{d_1} \notin \mathbb{Q}$, we get $b \neq 0$. Since $d_1 = a^2 + b^2 d + 2ab\sqrt{d}$, the linear independence of $(1, \sqrt{d}\,)$ implies $a = 0$ and $d_1 = b^2 d$.

2. If $\xi \in K \setminus \mathbb{Q}$ and Δ is the fundamental discriminant of ξ, then $\xi = u + v\sqrt{\Delta}$ for some u, $v \in \mathbb{Q}$ such that $v \neq 0$, and therefore $K = \mathbb{Q}(\sqrt{\Delta})$. Conversely, if $K = \mathbb{Q}(\sqrt{\Delta})$ for some fundamental discriminant Δ and $\xi \in K \setminus \mathbb{Q}$, then $\xi = u + v\sqrt{\Delta}$ for some u, $v \in \mathbb{Q}$ such that $v \neq 0$, and by Theorem 1.1.6.3 it follows that Δ is the fundamental discriminant of ξ. This proves the existence and uniqueness of Δ_K.

If Δ is any quadratic discriminant such that $K = \mathbb{Q}(\sqrt{\Delta}\,)$, then $\Delta = \Delta_K b^2$ for some $b \in \mathbb{Q}$ by 1., and Δ_K is the fundamental discriminant associated with Δ.

3. Suppose that $K = \mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Q}^\times$ is not a square, $\alpha = u + v\sqrt{d}$ and $\alpha_1 = u_1 + v_1\sqrt{d}$, where u, u_1, v, $v_1 \in \mathbb{Q}$. Then $\alpha' = u - v\sqrt{d}$, $\alpha_1' = u_1 - v_1\sqrt{d}$, and it is easily checked that $(\alpha + \alpha_1)' = \alpha' + \alpha_1'$ and $(\alpha\alpha_1)' = \alpha'\alpha_1'$. Moreover, $\iota \circ \iota = \mathrm{id}_K$ implies that ι is a field automorphism, and clearly $\iota \,|\, \mathbb{Q} = \mathrm{id}_\mathbb{Q}$.

If α, $\beta \in K$, then it follows that $\mathcal{N}(\alpha\beta) = \alpha\beta(\alpha\beta)' = \alpha\alpha'\beta\beta' = \mathcal{N}(\alpha)\mathcal{N}(\beta)$ and $\mathcal{T}(\alpha + \beta) = \alpha + \beta + (\alpha + \beta)' = \alpha + \alpha' + \beta + \beta' = \mathcal{T}(\alpha) + \mathcal{T}(\beta)$. □

1.2. The modular group

We consider the decomposition $\mathbb{C} \setminus \mathbb{Q} = \mathfrak{H}^+ \uplus \mathfrak{H}^- \uplus (\mathbb{R} \setminus \mathbb{Q})$, where

$$\mathfrak{H}^+ = \{z \in \mathbb{C} \mid \Im(z) > 0\} \quad \text{and} \quad \mathfrak{H}^- = \{z \in \mathbb{C} \mid \Im(z) < 0\}$$

denote the upper and the lower half-plane, respectively. We make use of the matrix groups

$$\mathsf{GL}_2(\mathbb{Z}) = \big\{A \in \mathsf{M}_2(\mathbb{Z}) \bigm| |\det(A)| = 1\big\} \quad \text{and}$$
$$\mathsf{SL}_2(\mathbb{Z}) = \big\{A \in \mathsf{M}_2(\mathbb{Z}) \bigm| \det(A) = 1\big\}\,,$$

we denote by $I \in \mathsf{SL}_2(\mathbb{Z})$ the unit matrix. Note that $\det\colon \mathsf{GL}_2(\mathbb{Z}) \to \{\pm 1\}$ is a group epimorphism with kernel $\mathsf{SL}_2(\mathbb{Z})$, and therefore $(\mathsf{GL}_2(\mathbb{Z}) : \mathsf{SL}_2(\mathbb{Z})) = 2$.

We define an operation

$$\mathsf{GL}_2(\mathbb{Z}) \times (\mathbb{C} \setminus \mathbb{Q}) \to \mathbb{C} \setminus \mathbb{Q}$$

by

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} z \;=\; \frac{\alpha z + \beta}{\gamma z + \delta} \quad \text{for all} \quad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathsf{GL}_2(\mathbb{Z}) \quad \text{and} \quad z \in \mathbb{C} \setminus \mathbb{Q}\,.$$

Theorem 1.2.1. *If A_1, $A \in \mathsf{GL}_2(\mathbb{Z})$ and $z \in \mathbb{C} \setminus \mathbb{Q}$, then $A_1(Az) = (A_1A)z$, $Iz = z$, $(-A)z = Az$, and*

$$\textit{if} \quad A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \quad \textit{then} \quad \Im(Az) = \frac{\det(A)}{|\gamma z + \delta|^2}\,\Im(z)\,.$$

In particular, the operation of $\mathsf{GL}_2(\mathbb{Z})$ on $\mathbb{C} \setminus \mathbb{Q}$ is a group operation, $\mathsf{GL}_2(\mathbb{Z})$ also operates on $\mathbb{R} \setminus \mathbb{Q}$, and $\mathsf{SL}_2(\mathbb{Z})$ operates both on $\mathfrak{H}^+$ and on $\mathfrak{H}^-$.

Proof. Obviously, $Iz = z$ and if $A \in \mathsf{GL}_2(\mathbb{Z})$, then $Az \in \mathbb{C} \setminus \mathbb{Q}$ for all $z \in \mathbb{C} \setminus \mathbb{Q}$, and $Az \in \mathbb{R} \setminus \mathbb{Q}$ for all $z \in \mathbb{R} \setminus \mathbb{Q}$. Assume now that

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \quad \text{and} \quad A_1 = \begin{pmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{pmatrix}.$$

Then

$$A_1(Az) = \frac{\alpha_1 \dfrac{\alpha z + \beta}{\gamma z + \delta} + \beta_1}{\gamma_1 \dfrac{\alpha z + \beta}{\gamma z + \delta} + \delta_1} = \frac{(\alpha_1 \alpha + \beta_1 \gamma) z + (\alpha_1 \beta + \beta_1 \delta)}{(\gamma_1 \alpha + \delta_1 \gamma) z + (\gamma_1 \beta + \delta_1 \delta)} = (A_1 A) z\,,$$

and therefore the operation of $\mathsf{GL}_2(\mathbb{Z})$ on $\mathbb{C} \setminus \mathbb{Q}$ and $\mathbb{R} \setminus \mathbb{Q}$ is a group operation. Moreover, we obtain

$$\begin{aligned} \Im(Az) &= \Im\Big(\frac{\alpha z + \beta}{\gamma z + \delta}\Big) = \Im\Big(\frac{(\alpha z + \beta)(\gamma \overline{z} + \delta)}{|\gamma z + \delta|^2}\Big) = \frac{\Im(\alpha \delta z + \beta \gamma \overline{z})}{|\gamma z + \Delta|^2} \\ &= \frac{\alpha \delta - \beta \gamma}{|\gamma z + \delta|^2}\, \Im(z) = \frac{\det(A)}{|\gamma z + \delta|^2}\, \Im(z)\,, \end{aligned}$$

and therefore $\mathsf{SL}_2(\mathbb{Z})$ operates both on $\mathfrak{H}^+$ and $\mathfrak{H}^-$. □

The transformation group $\mathfrak{M}$ induced by the operation of $\mathsf{SL}_2(\mathbb{Z})$ on $\mathfrak{H}^+$ is called the *modular group*. There is a natural epimorphism $\rho\colon \mathsf{SL}_2(\mathbb{Z}) \to \mathfrak{M}$, mapping a matrix $A \in \mathsf{SL}_2(\mathbb{Z})$ onto the transformation $z \mapsto Az$ of $\mathfrak{H}^+$. It follows by the subsequent Theorem 1.2.2 that $\operatorname{Ker}(\rho) = \{\pm I\}$, and therefore ρ induces an isomorphism $\rho^*\colon \mathsf{PSL}_2(\mathbb{Z}) = \mathsf{SL}_2(\mathbb{Z})/\{\pm I\} \overset{\sim}{\to} \mathfrak{M}$.

For $z \in \mathbb{C} \setminus \mathbb{Q}$, we denote by

$$\operatorname{Stab}(z) = \{S \in \mathsf{GL}_2(\mathbb{Z}) \mid Sz = z\} \quad \text{and} \quad \operatorname{Stab}^+(z) = \operatorname{Stab}(z) \cap \mathsf{SL}_2(\mathbb{Z})$$

the isotropy groups of z for the action of $\mathsf{GL}_2(\mathbb{Z})$ and $\mathsf{SL}_2(\mathbb{Z})$, respectively. We call $\operatorname{Stab}(z)$ the *stabilizer* and $\operatorname{Stab}^+(z)$ the *proper stabilizer* of z. By definition,

$$\{\pm I\} \subset \operatorname{Stab}^+(z) \subset \operatorname{Stab}(z) \subset \mathsf{GL}_2(\mathbb{Z})$$

are subgroups.

Theorem 1.2.2. *Let $z \in \mathbb{C} \setminus \mathbb{Q}$ be an irrational number.*

1. *If z is not a quadratic irrational, then* $\operatorname{Stab}(z) = \{\pm I\}$.
2. *If z is a quadratic irrational of type (a, b, c) and discriminant Δ, then*

$$\operatorname{Stab}(z) = \left\{ \begin{pmatrix} \frac12(x + by) & -cy \\ ay & \frac12(x - by) \end{pmatrix} \,\middle|\, x,\, y \in \mathbb{Z},\ |x^2 - \Delta y^2| = 4 \right\},$$

$$\operatorname{Stab}^+(z) = \left\{ \begin{pmatrix} \frac12(x + by) & -cy \\ ay & \frac12(x - by) \end{pmatrix} \,\middle|\, x,\, y \in \mathbb{Z},,\ x^2 - \Delta y^2 = 4 \right\}.$$

and $\operatorname{Stab}^+(z) \ne \operatorname{Stab}(z)$ *holds if and only if there exist $x, y \in \mathbb{Z}$ such that $x^2 - \Delta y^2 = -4$.*

PROOF. Assume that

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{Stab}(z)\,, \quad \text{hence} \quad z = \frac{\alpha z + \beta}{\gamma z + \delta}\,,$$

and $e = \det(A) = \alpha\delta - \beta\gamma \in \{\pm 1\}$. Then $\gamma z^2 + (\delta - \alpha)z - \beta = 0$, and since $z \notin \mathbb{Q}$, it follows that either $\gamma \neq 0$ and z is a quadratic irrational, or $\gamma = \beta = 0$ and $\alpha = \delta$. In the latter case, we obtain $A = \pm I$, which in particular proves 1.

Thus assume now that $\gamma \neq 0$, and let z be a quadratic irrational of type (a, b, c) and discriminant Δ. By Theorem 1.1.2.2 there is some $y \in \mathbb{Z}$ satisfying $\gamma = ay$, $\delta - \alpha = -by$, $-\beta = cy$, and consequently $\Delta y^2 = (\delta - \alpha)^2 + 4\beta\gamma = (\alpha + \delta)^2 - 4e$. We set $x = \alpha + \delta$ and obtain

$$A = \begin{pmatrix} \frac{1}{2}(x + by) & -cy \\ ay & \frac{1}{2}(x - by) \end{pmatrix}.$$

Since $4\det(A) = 4e = x^2 - \Delta y^2$, we get $|x^2 - \Delta y^2| = 4$, and $A \in \mathrm{Stab}^+(z)$ if and only if $x^2 - \Delta y^2 = 4$. It remains to prove that every matrix of this form lies in the stabilizer.

Thus let again z be a quadratic irrational of type (a, b, c) and discriminant Δ. Let x, $y \in \mathbb{Z}$ and $e \in \{\pm 1\}$ be such that $x^2 - \Delta y^2 = 4e$, and set

$$A = \begin{pmatrix} \frac{1}{2}(x + by) & -cy \\ ay & \frac{1}{2}(x - by) \end{pmatrix} \in \mathsf{M}_2(\mathbb{Q})\,.$$

Then

$$\det(A) = \frac{1}{4}(x^2 - b^2y^2) + acy^2 = \frac{1}{4}(x^2 - \Delta y^2) = e\,.$$

Now $x^2 - \Delta y^2 \equiv x^2 - b^2 y^2 \equiv 0 \bmod 4$ implies $x \equiv by \bmod 2$ and thus $A \in \mathsf{GL}_2(\mathbb{Z})$. We set

$$\alpha = \frac{1}{2}(x + by)\,, \quad \beta = -cy\,, \quad \gamma = ay\,, \quad \delta = \frac{1}{2}(x - by)\,,$$

and then we obtain

$$z - Az = \frac{\gamma z^2 + (\delta - \alpha)z - \beta}{\gamma z + \delta} = \frac{y(az^2 - bz + c)}{\gamma z + \delta} = 0\,. \qquad \square$$

For a quadratic discriminant Δ, the Diophantine equation

$$|x^2 - \Delta y^2| = 4$$

occuring in Theorem 1.2.2 is called *Pell's equation* and plays an important role in the theory of quadratic irrationals. Later, in Theorem 5.2.10, we shall obtain a deeper insight into the structure of the group $\mathrm{Stab}(\xi)$ using the theory of units in quadratic orders.

For negative quadratic discriminants, the theory of Pell's equation is simple. Indeed, suppose that $\Delta < 0$. Then the equation $x^2 - \Delta y^2 = -4$ has no solutions, and if

$$L = \{(x, y) \in \mathbb{Z}^2 \mid x^2 - \Delta y^2 = 4\}\,,$$

then it is easily verified that

$$L\cap\mathbb{N}^2=\begin{cases}\{(2,0)\} & \text{if}\quad \Delta<-4\,,\\ \{(1,1)\,,\,(2,0)\} & \text{if}\quad \Delta=-3\,,\\ \{(0,1)\,,\,(2,0)\} & \text{if}\quad \Delta=-4\,,\end{cases}\quad\text{and}\quad |L|=\begin{cases}2 & \text{if}\quad \Delta<-4\,,\\ 6 & \text{if}\quad \Delta=-3\,,\\ 4 & \text{if}\quad \Delta=-4\,.\end{cases}$$

If $\mathbb{W}_n$ denotes the group of n-th roots of unity in $\mathbb{C}$, then

$$\Big\{\frac{x+y\sqrt{\Delta}}{2}\;\Big|\;(x,y)\in L\Big\}=\begin{cases}\mathbb{W}_2=\langle -1\rangle & \text{if}\quad \Delta<-4\,,\\ \mathbb{W}_6=\langle -\zeta_3\rangle & \text{if}\quad \Delta=-3\,,\\ \mathbb{W}_4=\langle \mathsf{i}\rangle & \text{if}\quad \Delta=-4\,.\end{cases}$$

For quadratic discriminants $\Delta>0$, the equation $x^2-\Delta y^2=4$ has infinitely many solutions $(x,y)\in\mathbb{Z}^2$. In contrast, *Pell's minus equation* $x^2-\Delta y^2=-4$ may have no integral solutions. A thorough theory of the structure of the solutions of Pell's equation will be given in Theorem 2.2.9 using the theory of continued fractions. The importance of Pell's equation for the theory of quadratic irrationals will become lucid in Theorem 1.3.8 and, even more definite, in Chapter 5 when we study unit groups and ideal class groups of quadratic orders, and in Chapter 6 when we investigate the equivalence of binary quadratic forms.

Before we proceed with the investigation of the modular group, we give an ad hoc proof of the fact that Pell's equation for positive quadratic discriminants has infinitely many solutions using Dirichlet's approximation theorem. It is obviously sufficient to prove that, for every $d\in\mathbb{N}$ which is not square, the Diophantine equation

$$x^2-dy^2=1$$

has infinitely many solutions $(x,y)\in\mathbb{Z}^2$ (this seemingly more simple Diophantine equation is called Pell's equation, too).

Theorem 1.2.3.

1. (Dirichlet's approximation theorem) *For every* $\alpha\in\mathbb{R}$ *and* $N\in\mathbb{N}$, *there exists some* $(p,q)\in\mathbb{Z}\times\mathbb{N}$ *such that*

$$\Big|\alpha-\frac{p}{q}\Big|<\frac{1}{qN}\quad\textit{and}\quad q\le N\,.$$

2. *For every* $\alpha\in\mathbb{R}\setminus\mathbb{Q}$, *there exist infinitely many pairs* $(p,q)\in\mathbb{Z}\times\mathbb{N}$ *such that* $(p,q)=1$ *and*

$$\Big|\alpha-\frac{p}{q}\Big|<\frac{1}{q^2}\,.$$

3. (Pell's Equation) *If* $d\in\mathbb{N}$ *is not a square, then there exist infinitely many pairs* $(x,y)\in\mathbb{N}^2$ *such that* $x^2-dy^2=1$.

Proof. 1. For $n\in[1,N]$, we set $\{\alpha n\}=\alpha n-\lfloor\alpha n\rfloor\in[0,1)$, and we consider the partition

$$[0,1)\;=\;\biguplus_{j=1}^{N}\Big[\frac{j-1}{N},\frac{j}{N}\Big)$$

of interval $[0,1)$ into N subintervals. By Dirichlet's box principle, there exist integers $n_1,\ n_2 \in [0,N]$ and $j \in [1,N]$ such that $n_1 < n_2$ and

$$\{\alpha n_1\},\ \{\alpha n_2\} \in \Big[\frac{j-1}{N}, \frac{j}{N}\Big)\,.$$

We set $q = n_2 - n_1$ and $p = \lfloor \alpha n_2 \rfloor - \lfloor \alpha n_1 \rfloor$. Then it follows that $q \in [1,N],\ \ p \in \mathbb{Z}$,

$$|\alpha q - p| = |\{\alpha n_2\} - \{\alpha n_1\}| < \frac{1}{N}\,, \quad \text{and therefore} \quad \Big|\alpha - \frac{p}{q}\Big| < \frac{1}{qN}\,.$$

2. Suppose that $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. For every $n \in \mathbb{N}$, it follows by 1. that there exists some $(p_n, q_n) \in \mathbb{Z} \times \mathbb{N}$ such that $q_n \le n$ and

$$\Big|\alpha - \frac{p_n}{q_n}\Big| < \frac{1}{nq_n} \le \frac{1}{q_n^2}\,.$$

We may assume that $(p_n, q_n) = 1$, and we assert that $\{q_n \mid n \in \mathbb{N}\}$ is infinite. Assume the contrary. Then there exist some $q \in \mathbb{N}$ and an infinite set $T \subset \mathbb{N}$ such that $q_n = q$ for all $n \in T$. We may assume that $N = \min(T) \ge 2$. Since

$$\Big|\frac{p_n}{q} - \frac{p_N}{q}\Big| \le \Big|\alpha - \frac{p_n}{q}\Big| + \Big|\alpha - \frac{p_N}{q}\Big| < \frac{1}{qn} + \frac{1}{qN} < \frac{1}{q} \quad \text{for all } n \in T,$$

it follows that $p_n = p_N = p$ (say) for all $n \in T$, and therefore

$$\Big|\alpha - \frac{p}{q}\Big| < \frac{1}{qn} \quad \text{for all } n \in T\,, \quad \text{whence} \quad \alpha = \frac{p}{q} \in \mathbb{Q}\,, \quad \text{a contradiction.}$$

3. If $d \in \mathbb{N}$ is not a square, then it follows by 2. that there exist infinitely many pairs $(x,y) \in \mathbb{Z} \times \mathbb{N}$ such that

$$\Big|\sqrt{d} - \frac{x}{y}\Big| < \frac{1}{y^2}\,. \tag{1}$$

Note that (1) implies that $x > 0$ and

$$\frac{x}{y} \le \sqrt{d} + \Big|\sqrt{d} - \frac{x}{y}\Big| < \sqrt{d} + \frac{1}{y^2} \le \sqrt{d} + 1\,.$$

Hence we obtain

$$0 < |x^2 - dy^2| = |x - y\sqrt{d}|(x + y\sqrt{d}) < \frac{1}{y}(x + y\sqrt{d}) = \frac{x}{y} + \sqrt{d} \le 2\sqrt{d} + 1\,.$$

By Dirichlet's box principle, there exist integers $k \in \mathbb{N}$ and $a,\ b \in [0, k-1]$ such that $k < 2\sqrt{d} + 1$, and the set

$$L = \{(x,y) \in \mathbb{N}^2 \mid x^2 - dy^2 = k,\ x \equiv a \mod k \ \text{ and } \ y \equiv b \mod k\,\}$$

is infinite. Now we fix some $(x_0, y_0) \in L$ and construct for every $(x,y) \in L$ a pair $(u,v) \in \mathbb{Z}^2$ such that $u^2 - dv^2 = 1$ in the following way.

For $(x,y) \in L$, we calculate

$$(x \pm y\sqrt{d})(x_0 \mp y_0\sqrt{d}) = (xx_0 - yy_0d) \pm (x_0y - xy_0)\sqrt{d}\,,$$

$xx_0 - yy_0d \equiv a^2 - b^2d \equiv 0 \mod k$ and $x_0y - xy_0 \equiv ab - ab \equiv 0 \mod k$. Hence there exist $u,\ v \in \mathbb{Z}$ such that

$$xx_0 - yy_0d = ku \quad \text{and} \quad x_0y - xy_0 = kv\,, \tag{2}$$

we obtain

$$\begin{aligned}k^2 &= (x^2-y^2d)(x_0^2-y_0^2d) = (x+y\sqrt{d})(x_0-y_0\sqrt{d})(x-y\sqrt{d})(x_0+y_0\sqrt{d})\\ &= k^2(u+v\sqrt{d})(u-v\sqrt{d}) = k^2(u^2-v^2d)\,, \quad \text{and therefore} \quad u^2-v^2d=1\,.\end{aligned}$$

By (2) it follows that

$$\begin{aligned}k(x_0u+dy_0v) &= x_0(xx_0-yy_0d)+dy_0(x_0y-xy_0) = x(x_0^2-dy_0^2) = kx\,,\\ k(y_0u+x_0v) &= y_0(xx_0-yy_0d)+x_0(x_0y-xy_0) = y(x_0^2-dy_0^2) = ky\,,\end{aligned}$$

and therefore $x = x_0u+dy_0v$ and $y = y_0u+x_0v$. Hence distinct pairs (x,y) yield distinct pairs (u,v), and thus we get in this way infinitely many pairs $(u,v) \in \mathbb{Z}^2$ (and thus also in $\mathbb{N}^2$) satisfying $u^2-dv^2=1$. □

Exercise 1.2.4. For a quadratic discriminant Δ, prove the following assertions:

- If the Diophantine equation $x^2-\Delta y^2 = -1$ has a solution $(x,y)\in\mathbb{N}^2$, then it has infinitely many solutions.
- If one of the Diophantine equations $x^2-\Delta y^2 = \pm 4$ has a solution in coprime integers $x,\ y\in\mathbb{Z}$, then $\Delta \equiv 5 \bmod 8$, and that equation has infinitely many such solutions.

The group operations of $\mathsf{GL}_2(\mathbb{Z})$ and $\mathsf{SL}_2(\mathbb{Z})$ on $\mathbb{C}\setminus\mathbb{Q}$ cause the following equivalence relations. Two complex numbers $z_1,\ z_2\in\mathbb{C}\setminus\mathbb{Q}$ are called

- *equivalent*, $z_1\sim z_2$, if $z_2 = Az_1$ for some $A\in\mathsf{GL}_2(\mathbb{Z})$;
- *properly equivalent*, $z_1\sim_+ z_2$, if $z_2 = Az_1$ for some $A\in\mathsf{SL}_2(\mathbb{Z})$.

Equivalence and proper equivalence are equivalence relations on $\mathbb{C}\setminus\mathbb{Q}$, and also on $\mathbb{C}\setminus\mathbb{R}$ and on $\mathbb{R}\setminus\mathbb{Q}$. Any two properly equivalent complex numbers $z_1,\ z_2\in\mathbb{C}\setminus\mathbb{Q}$ are equivalent. By Theorem 1.2.1, two equivalent complex numbers $z_1,\ z_2\in\mathbb{C}\setminus\mathbb{R}$ are properly equivalent if and only if they lie in the same half-plane.

The investigation of these equivalence relations depends on the study of suitable generators for the groups $\mathsf{GL}_2(\mathbb{Z})$ and $\mathsf{SL}_2(\mathbb{Z})$. We define the matrices

$$U = \begin{pmatrix}-1 & 0\\ 0 & 1\end{pmatrix}, \quad S = \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} \quad \text{and} \quad T = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}.$$

It is easily checked that

$$\mathsf{GL}_2(\mathbb{Z}) = \mathsf{SL}_2(\mathbb{Z}) \uplus \mathsf{SL}_2(\mathbb{Z})U\,, \quad U^2 = I\,, \quad S^2 = (ST)^3 = (TS)^3 = -I\,,$$

and if $z\in\mathbb{C}\setminus\mathbb{Q}$, then $Uz=-z$, $Sz = -z^{-1}$ and $T^nz = z+n$ for all $n\in\mathbb{Z}$. Consequently, if $z_1,\ z_2\in\mathbb{C}\setminus\mathbb{Q}$ are equivalent but not properly equivalent, then z_1 and $Uz_2 = -z_2$ are properly equivalent.

The set

$$\mathcal{F} = \Bigl\{z\in\mathfrak{H}^+ \Bigm| |z|>1,\ -\frac{1}{2} < \Re(z) \le \frac{1}{2} \quad \text{or} \quad |z|=1,\ 0\le \Re(z)\le\frac{1}{2}\Bigr\}$$

is called the *fundamental domain* of the modular group, a terminology which is justified by the subsequent Theorem 1.2.5.

Theorem 1.2.5. $\mathsf{SL}_2(\mathbb{Z}) = \langle S,T\rangle$, $\mathsf{GL}_2(\mathbb{Z}) = \langle U,S,T\rangle$, *and for every* $z \in \mathbb{C}\setminus\mathbb{R}$ *there exists a unique* $z_0 \in \mathcal{F}$ *such that* $z \sim z_0$.

Proof. We consider the following two assertions **A** and **B**.

A. For every $z \in \mathfrak{H}^+$ there is some $B \in \langle S,T\rangle$ such that $Bz \in \mathcal{F}$.

B. If z, $z_1 \in \mathcal{F}$ are equivalent, then $z = z_1$.

We first finish the proof of our theorem using **A** and **B**.

We prove first that for every $z \in \mathbb{C}\setminus\mathbb{R}$ there exists a unique $z_0 \in \mathcal{F}$ such that $z \sim z_0$. If $z \in \mathfrak{H}^+$, then by **A** there exists some $B \in \langle S,T\rangle$ such that $z_0 = Bz \in \mathcal{F}$. If $z \in \mathfrak{H}^-$, then $-z \in \mathfrak{H}^+$, and again by **A** there exists some $B \in \langle S,T\rangle$ such that $z_0 = B(-z) = BUz \in \mathcal{F}$. Hence $z \sim z_0$, and if $z_1 \in \mathcal{F}$ is any number satisfying $z \sim z_1$, then $z_1 \sim z_0$ and thus $z_1 = z_0$ by **B**.

For the proof of $\mathsf{SL}_2(\mathbb{Z}) = \langle S,T\rangle$ and $\mathsf{GL}_2(\mathbb{Z}) = \langle U,S,T\rangle$, it suffices to show that $\mathsf{SL}_2(\mathbb{Z}) \subset \langle S,T\rangle$. Suppose that $A \in \mathsf{SL}_2(\mathbb{Z})$, and let $z \in \mathcal{F}$ be not a quadratic irrational. Then $A^{-1}z \in \mathfrak{H}^+$, by **A** there is some $B \in \langle S,T\rangle$ such that $BA^{-1}z \in \mathcal{F}$, and since $BA^{-1}z \sim z$, it follows by **B** that $BA^{-1}z = z$. By Theorem 1.2.2, we obtain $BA^{-1} = \pm I$, and consequently $A = \pm B \in \{B,\, S^2B\} \subset \langle S,T\rangle$.

Proof of **A.** Suppose that $z \in \mathfrak{H}^+$. We assert that for every $M \in \mathbb{R}_{>0}$ the set

$$\big\{(\gamma,\delta) \in \mathbb{Z}^2 \;\big|\; |\gamma z+\delta| \le M\big\}$$

is finite. Indeed, if $M \in \mathbb{R}_{>0}$ and $(\gamma,\delta) \in \mathbb{Z}^2$ is such that $|\gamma z+\delta| \le M$, then $\Im(z)|\gamma| = |\Im(\gamma z+\delta)| \le |\gamma z+\delta| \le M$, hence $|\gamma| \le \Im(z)^{-1}M$, and $|\delta| \le M + |\gamma z|$.

Now it follows that there exists some matrix

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \langle S,T\rangle$$

such that

$$|\gamma z+\delta| \le |\gamma_1 z+\delta_1| \quad \text{for all matrices} \quad A_1 = \begin{pmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{pmatrix} \in \langle S,T\rangle\,,$$

and therefore (by Theorem 1.2.1)

$$\Im(Az) = \frac{\Im(z)}{|\gamma z+\delta|^2} \ge \frac{\Im(z)}{|\gamma_1 z+\delta_1|^2} = \Im(A_1z) \quad \text{for all matrices } A_1 \in \langle S,T\rangle.$$

Let $n \in \mathbb{Z}$ be such that

$$-n-\frac12 < \Re(Az) \le -n+\frac12\,, \quad \text{and set } z_1 = T^nAz.$$

Then

$$-\frac12 < \Re(z_1) \le \frac12\,, \quad Sz_1 = ST^nAz \quad \text{and} \quad ST^nA \in \langle S,T\rangle\,.$$

Hence it follows that

$$\Im(Sz_1) = \frac{\Im(z_1)}{|z_1|^2} \le \Im(Az) = \Im(z_1)\,, \quad \text{and therefore} \quad |z_1| \ge 1\,.$$

If $z_1 \in \mathcal{F}$, then $B = T^nA \in \langle S,T\rangle$, $Bz \in \mathcal{F}$, and we are done. Thus suppose that $z_1 \notin \mathcal{F}$. Then

$$|z_1| = 1 \;\text{ and }\; -\frac12 < \Re(z_1) < 0\,.$$

Since $|Sz_1| = |z_1| = 1$, and $\Re(Sz_1) = -\Re(z_1)$, it follows that $Sz_1 \in \mathcal{F}$, and if $B = ST^nA$, then $B \in \langle S, T\rangle$ and $Bz \in \mathcal{F}$. □[**A.**]

Proof of **B.** Let z, $z_1 \in \mathcal{F}$ be equivalent. Then they are properly equivalent, and there is some $A \in \mathsf{SL}_2(\mathbb{Z})$ such that $z_1 = Az$, say

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \quad \text{where} \quad \alpha\delta - \beta\gamma = 1\,.$$

Since $(-A)z = Az$, we may assume that $\gamma \geq 0$, and $\delta > 0$ if $\gamma = 0$. Moreover, we may assume that

$$\Im(z_1) = \frac{\Im(z)}{|\gamma z + \delta|^2} \geq \Im(z) > 0\,, \quad \text{and therefore} \quad |\gamma z + \delta| \leq 1\,.$$

Since

$$|z| \geq 1 \quad \text{and} \quad \Re(z) \geq -\frac{1}{2}\,,$$

we obtain

$$1 \geq |\gamma z + \delta|^2 = \gamma^2|z|^2 + 2\Re(z)\gamma\delta + \delta^2 \geq \gamma^2 - |\gamma\delta| + \delta^2 = \Bigl(\gamma - \frac{|\delta|}{2}\Bigr)^2 + \frac{3\delta^2}{4}\,.$$

This is only possible for $\delta \in \{0, \pm 1\}$.

CASE 1: $\delta = 0$. Then $\gamma^2 \leq 1$, hence $\gamma = 1$ and $\det(A) = -\beta = 1$. Since

$$z_1 = \alpha - \frac{1}{z} \quad \text{and} \quad \Im(z_1) = \frac{\Im(z)}{|z|^2} \geq \Im(z)\,,$$

it follows that $|z| = 1$ and $\Im(z_1) = \Im(z)$. On the other hand,

$$\alpha = z_1 + z^{-1} = z_1 + \overline{z} = \Re(z_1) + \Re(z) \in \mathbb{Z} \quad \text{and} \quad \{\Re(z), \Re(z_1)\} \subset \Bigl(-\frac{1}{2}, \frac{1}{2}\Bigr]\,,$$

hence $\Re(z) = \Re(z_1)$ and therefore $z = z_1$.

CASE 2: $|\delta| = 1$. Then

$$\Bigl(\gamma - \frac{1}{2}\Bigr)^2 \leq \frac{1}{4}\,, \quad \text{hence} \quad \gamma \in \{0, 1\}\,, \quad \text{and} \quad \gamma = 1 \;\text{ if }\; \delta = -1\,.$$

CASE 2a: $\delta = 1$. We assert that $\gamma = 0$. Indeed, suppose to the contrary that $\gamma = 1$. Then $|1 + z| \leq 1$ and therefore $1 \geq (z+1)(\overline{z}+1) = |z|^2 + 2\Re(z) + 1$, hence $2\,\Re(z) \leq -|z|^2 \leq -1$ and $z \notin \mathcal{F}$, a contradiction.

Since $\gamma = 0$ and $\delta = 1$, we obtain $\alpha = 1$ and $z_1 = z + \beta$. Now it follows that

$$\Re(z_1) = \Re(z) + \beta \quad \text{and} \quad \{\Re(z), \Re(z_1)\} \subset \Bigl(-\frac{1}{2}, \frac{1}{2}\Bigr]\,,$$

which implies $\beta = 0$ and $z = z_1$.

CASE 2b: $\delta = -1$. Then $\gamma = 1$, $-\alpha - \beta = 1$ and $|z - 1| = |\gamma z + \delta| \leq 1$. Since $1 \geq |z - 1|^2 = (z-1)(\overline{z}-1) = |z|^2 - 2\,\Re(z) + 1$, we obtain $2\,\Re(z) \geq |z|^2 \geq 1$, and

$$\Re(z) \in \Bigl(-\frac{1}{2}, \frac{1}{2}\Bigr] \quad \text{implies} \quad |z| = 1 \;\text{ and }\; \Re(z) = \frac{1}{2}\,.$$

Hence it follows that

$$z = \frac{1+\sqrt{-3}}{2} \quad \text{and}$$

$$z_1 = Az = \frac{\alpha z + \beta}{z-1} = \frac{\alpha(z-1) + (\alpha+\beta)}{z-1} = \alpha + \frac{-1}{z-1} = \alpha + z\,.$$

But, as z, $z_1 \in \mathcal{F}$, we obtain

$$\{\Re(z),\, \Re(z_1)\} \subset \Big(-\frac{1}{2}, \frac{1}{2}\Big], \quad \text{and therefore} \quad \alpha = 0 \;\text{ and }\; z = z_1\,. \qquad \square$$

Exercise 1.2.6. A subset Γ of the upper half-plane is called a *generalized circle* if there exist a, $c \in \mathbb{R}$ and $b \in \mathbb{C}$ such that

$$|b|^2 - ac > 0 \quad \text{and} \quad \Gamma = \{ z \in \mathfrak{H}^+ \mid a|z|^2 + \Re(bz) + c = 0 \}\,.$$

Justify this terminology, and prove: If $A \in \mathsf{SL}_2(\mathbb{Z})$ and Γ is a generalized circle, then its image under the modular group $\{Az \mid z \in \Gamma\}$ is again a generalized circle.

Exercise 1.2.7. Prove that the following algorithm terminates after a finite number of steps and transforms a number of the upper half-plane into an equivalent number of the fundamental domain.

```
Input $z \in \mathfrak{H}^+$.
Step 1. If $n \in \mathbb{Z}$ is such that $-n - \frac{1}{2} < \Re(z) \le -n + \frac{1}{2}$, set $z \leftarrow T^n z$
        and go to Step 2.
Step 2. If either $|z| > 1$, or $|z| = 1$ and $0 \le \Re(z) \le \frac{1}{2}$, output $z$ and
        terminate the algorithm.
        If $|z| = 1$ and $-\frac{1}{2} < \Re(z) < 0$, set $z \leftarrow Sz$, output $z$ and ter-
        minate the algorithm.
        If $|z| < 1$, set $z \leftarrow Sz$, and go to Step 1.
```

Apply the algorithm to the number

$$z = -\frac{3+2\mathsf{i}}{8+6\mathsf{i}} \quad \text{(see Exercise 1.1.3)}$$

and determine some $A \in \mathsf{SL}_2(\mathbb{Z})$ such that $Az \in \mathcal{F}$.

Theorem 1.2.8. *Let ξ be a quadratic irrational of discriminant Δ. Then every complex number equivalent to ξ is also a quadratic irrational of discriminant Δ.*

Proof. Let $\mathfrak{G}$ be the set of all $A \in \mathsf{GL}_2(\mathbb{Z})$ with the property that for every quadratic irrational η of discriminant Δ the number $A\eta$ is also a quadratic irrational of discriminant Δ. Then $\mathfrak{G}$ is a subgroup of $\mathsf{GL}_2(\mathbb{Z})$, and by Theorem 1.2.5 it suffices to prove that $\{U, S, T\} \subset \mathfrak{G}$. Since $U\xi = -\xi$, $S\xi = -\xi^{-1}$ and $T\xi = \xi + 1$, this follows by Lemma 1.1.4. $\square$

Exercise 1.2.9. Give a straightforward proof of Theorem 1.2.8 without using Theorem 1.2.5.

1.3. Reduced quadratic irrationals

We shall see in Theorem 1.3.10 that for each quadratic discriminant Δ there are only finitely many (proper) equivalence classes of quadratic irrationals with discriminant Δ, and we shall explicitly give representatives for them. In the literature, this procedure is usually called *reduction*, and is mostly described either in the language of binary quadratic forms or in the language of ideals in quadratic orders. According to our program considering quadratic irrationals as the most fundamental concept, we first define and investigate reduced quadratic irrationals.

Definition 1.3.1. A quadratic irrational ξ is called *reduced* if

- either $\xi \in \mathcal{F}$
- or $\xi \in \mathbb{R}_{>1}$ and $-1 < \xi' < 0$.

In this section, we characterize reduced quadratic irrationals and state that they indeed represent all proper equivalence classes (see Theorem 1.3.2 for negative discriminants and Theorem 1.3.5 for positive discriminants). For negative discriminants, this turns out to be rather simple. For positive discriminants however, we must postpone the completion of the proof to Section 2.2.

In Theorem 1.3.8, we investigate the connection between equivalence and proper equivalence, which is closely connected with Pell's equation.

Finally, in Theorem 1.3.10, we state that there are only finitely many (proper) equivalence classes of quadratic irrationals of fixed discriminant, and we introduce the all-important notion of a (narrow) class number. In Chapter 5 these class numbers will occur as ideal class numbers of quadratic orders, and in Chapter 6 they will occur as class numbers for the composition class groups of binary quadratic forms. In Chapter 8, we shall prove Dirichlet's analytic class number formula.

Theorem 1.3.2. *Let ξ be a quadratic irrational of type (a,b,c) and discriminant $\Delta < 0$.*

1. *There exists a uniquely determined reduced quadratic irrational ξ_0 which is equivalent to ξ.*
2. *ξ is reduced if and only if either $-a < b \le a < c$ or $0 \le b \le a = c$. In particular, if ξ is reduced, then*

$$0 < a \le \sqrt{\frac{|\Delta|}{3}} \quad \textit{and} \quad |b| \le a\,.$$

3. *The basis number ω_Δ is reduced.*

Proof. 1. By Theorem 1.2.5 there exists a unique $\xi_0 \in \mathcal{F}$ such that $\xi_0 \sim \xi$, and by Theorem 1.2.8 every complex number equivalent to ξ is a quadratic irrational.

2. ξ is reduced if and only if $\xi \in \mathcal{F}$, that is, if and only if $\Im(\xi) > 0$ and

$$\text{either } |\xi| > 1 \text{ and } -\frac{1}{2} < \Re(\xi) \le \frac{1}{2}, \quad \text{or } |\xi| = 1 \text{ and } 0 \le \Re(\xi) \le \frac{1}{2}\,.$$

By the very definition of the type we have $a \ne 0$, $(a,b,c)=1$, $b^2-4ac<0$,

$$\xi = \frac{b+\sqrt{b^2-4ac}}{2a}, \quad \Re(\xi) = \frac{b}{2a}, \quad \Im(\xi) = \frac{\sqrt{4ac-b^2}}{2a} \quad \text{and} \quad |\xi|^2 = \frac{c}{a}\,.$$

Consequently, ξ is reduced if and only if $a>0$ and

$$\text{either} \quad c>a \ \text{ and } \ -\frac{1}{2} < \frac{b}{2a} \le \frac{1}{2}\,, \quad \text{or} \quad c=a \ \text{ and } \ 0 \le \frac{b}{2a} \le \frac{1}{2}\,.$$

Hence ξ is reduced if and only if either $-a<b\le a<c$ or $0\le b\le a=c$. In particular, if ξ is reduced, then $|b|\le a$ and $c\ge a>0$, which implies

$$-\Delta = 4ac-b^2 \ge 4a^2-a^2 = 3a^2 \quad \text{and} \quad 0<a\le \sqrt{\frac{-\Delta}{3}} = \sqrt{\frac{|\Delta|}{3}}\,.$$

3. If $\Delta = 4D+\sigma_\Delta$, where $D\in\mathbb{Z}$ and $\sigma_\Delta\in\{0,1\}$, then ω_Δ is of type $(1,\sigma_\Delta,-D)$, and thus it is reduced by 2. ☐

Example 1.3.3. 1. If $\Delta\in\{-3,-7,-11,-19,-27,-43,-67,-163\}$, then the basis number ω_Δ is the only reduced quadratic irrational of discriminant Δ.

We give details in the most complicated case $\Delta=-163$ and leave the others as an exercise. Let ξ be a reduced quadratic irrational of type (a,b,c) and discriminant $b^2-4ac=-163$. Then b is odd, $0<a\le 7=\lfloor\sqrt{163/3}\rfloor$, and either $-a<b\le a\le c$ or $0\le b\le a=c$ by Theorem 1.3.10. It follows that $b^2\in\{1,9,25,49\}$. If $b^2=1$, then $ac=41$, and $(a,b,c)=(1,1,41)$. If $b^2\in\{9,25,49\}$, then $ac\in\{43,47,53\}$, which is impossible.

2. If $\Delta=4D$ and $D\in\{-1,-2,-3,-4,-7\}$, then the basis number $\omega_\Delta=\mathrm{i}\sqrt{D}$ is the only reduced quadratic irrational of discriminant Δ. This again is left as an exercise.

Exercise 1.3.4. Determine all reduced quadratic irrationals of discriminant $\Delta\in[-28,-3]\cup\{-43,-67\}$.

For a real quadratic irrational ξ, we define its *successor* $\xi^\#$ by

$$\xi^\# = \begin{pmatrix} 0 & 1 \\ 1 & -\lfloor\xi\rfloor \end{pmatrix}\xi \;=\; \frac{1}{\xi-\lfloor\xi\rfloor}\,.$$

This definition is justified by the role of $\xi^\#$ in the theory of continued fractions (see Theorem 2.1.3).

Theorem 1.3.5. *Let ξ be a quadratic irrational of type (a,b,c) and discriminant $\Delta>0$.*

1. *ξ is properly equivalent to a reduced quadratic irrational.*
2. *The following assertions are equivalent:*
   - (a) *ξ is reduced.*
   - (b) *$-\xi'^{-1}$ is reduced.*
   - (c) $0<\sqrt{\Delta}-b<2a<\sqrt{\Delta}+b$.
   - (d) $0<\sqrt{\Delta}-b<-2c<\sqrt{\Delta}+b$.

3. *Let* ξ *be reduced.*
   (a) $0 < a < \sqrt{\Delta}$, $0 < b < \sqrt{\Delta}$, $0 < -c < \sqrt{\Delta}$ *and* $\xi < \sqrt{\Delta}$.
   (b) *The numbers* $\xi^{\#}$ *and* $\eta = -\xi' + \lfloor \xi \rfloor$ *are also reduced quadratic irrationals of discriminant* Δ, *and* η *is the unique reduced quadratic irrational satisfying* $\eta^{\#} = -\xi'^{-1}$.

Proof. 1. This will be proved (using the theory of continued fractions) in Theorem 2.2.2.3.

2. By definition, ξ is reduced if and only if $\xi > 1$ and $-1 < \xi' < 0$. These conditions are equivalent to $-\xi'^{-1} > 1$ and $-1 < -\xi^{-1} = (-\xi'^{-1})' < 0$, which means that $-\xi'^{-1}$ is reduced. Hence (a) and (b) are equivalent. Since $-\xi'^{-1}$ is of type $(-c, b, -a)$, it remains to prove the equivalence of (a) and (c). Observe that

$$\xi = \frac{b+\sqrt{\Delta}}{2a}, \quad \xi' = \frac{b-\sqrt{\Delta}}{2a} \quad \text{and} \quad \xi - \xi' = \frac{\sqrt{\Delta}}{a}.$$

If $a < 0$, then $\xi - \xi' < 0$ and thus ξ is not reduced. If $a > 0$, we obtain:

$$\begin{aligned} \xi \text{ is reduced} &\iff -1 < \frac{b-\sqrt{\Delta}}{2a} < 0 \quad \text{and} \quad 1 < \frac{b+\sqrt{\Delta}}{2a} \\ &\iff -2a < b - \sqrt{\Delta} < 0 \quad \text{and} \quad 2a < b + \sqrt{\Delta} \\ &\iff 0 < \sqrt{\Delta} - b < 2a < \sqrt{\Delta} + b\,. \end{aligned}$$

Hence (a) and (c) are equivalent.

3. (a) By 2.(c) and 2.(d) we obtain $0 < b < \sqrt{\Delta}$, $0 < 2a < \sqrt{\Delta} + b < 2\sqrt{\Delta}$ and $0 < -2c < \sqrt{\Delta} + b < 2\sqrt{\Delta}$. Hence it follows that $0 < a < \sqrt{\Delta}$, $0 < -c < \sqrt{\Delta}$ and $\xi < \sqrt{\Delta}$.

(b) By Lemma 1.1.4, $\xi^{\#}$ and $-\xi' + \lfloor \xi \rfloor$ are quadratic irrationals of discriminant Δ. Now $0 < \xi - \lfloor \xi \rfloor < 1$ implies $\xi^{\#} = (\xi - \lfloor \xi \rfloor)^{-1} > 1$, and $\xi' - \lfloor \xi \rfloor \le \xi' - 1 < -1$ implies $-1 < (\xi^{\#})' = (\xi' - \lfloor \xi \rfloor)^{-1} < 0$. Hence $\xi^{\#}$ is reduced.

Since $\eta = -\xi' + \lfloor \xi \rfloor > \lfloor \xi \rfloor \ge 1$ and $\eta' = -\xi + \lfloor \xi \rfloor \in (-1, 0)$, it follows that η is reduced, $\lfloor \eta \rfloor = \lfloor \xi \rfloor$, and $\eta^{\#} = (\eta - \lfloor \eta \rfloor)^{-1} = (\eta - \lfloor \xi \rfloor)^{-1} = -\xi'^{-1}$.

Assume now that η_1 is any reduced quadratic irrational such that $\eta_1^{\#} = -\xi'^{-1}$. Then we obtain $-\xi' = \eta_1 - \lfloor \eta_1 \rfloor$, hence $\eta_1 = \lfloor \eta_1 \rfloor - \xi'$, and $-1 < \eta_1' = \lfloor \eta_1 \rfloor - \xi < 0$. From this, it follows that $\lfloor \eta_1 \rfloor = \lfloor \xi \rfloor$, and $\eta_1 = -\xi' + \lfloor \xi \rfloor = \eta$. □

Exercise 1.3.6. Let ξ be a reduced quadratic irrational of type (a, b, c) and discriminant $\Delta > 0$. Suppose that $n = \lfloor \xi \rfloor$ and $m = \lfloor -\xi'^{-1} \rfloor$. Prove that

- the successor $\xi^{\#}$ of ξ is of type $(bn - an^2 - c, -b + 2an, -a)$, and
- there is a unique reduced quadratic irrational $\xi^{\flat}$ satisfying $(\xi^{\flat})^{\#} = \xi$. It is of type $(-c, -b - 2cm, -a - bm - cm^2)$.

Theorem 1.3.5 allows us to determine all reduced quadratic irrationals of a given positive discriminant. However, it provides no criterion to decide whether two (reduced) real quadratic irrationals are equivalent. Such a criterion, even valid for all irrational real numbers, will be given in Chapter 2 by the equivalence theorem (see Theorem 2.1.14).

Exercise 1.3.7. Determine all reduced quadratic irrationals of discriminant $\Delta \in [5, 32]$ (as already mentioned, at the moment we have no criterion to group them into (proper) equivalence classes, but we will do this as soon as we have proved the equivalence theorem, see Exercise 2.1.15).

Theorem 1.3.8. *For a quadratic discriminant Δ, the following assertions are equivalent*:

(a) *Any two equivalent quadratic irrationals of discriminant Δ are properly equivalent.*

(b) *Some [every] quadratic irrational ξ of discriminant Δ is properly equivalent to $-\xi$.*

(c) *There exists some $(x, y) \in \mathbb{Z}^2$ such that $x^2 - \Delta y^2 = -4$.*
If this condition is fulfilled, we say that *Pell's minus equation for Δ has integral solutions.*

Proof. (a) $\Rightarrow$ (b) If ξ is any quadratic irrational of discirminant Δ, then ξ is equivalent to $-\xi$, and thus ξ is properly equivalent to $-\xi$.

(b) $\Rightarrow$ (c) Let ξ be a quadratic irrational of discriminant Δ which is properly equivalent to $-\xi$, say $-\xi = A\xi$ for some $A \in \mathsf{SL}_2(\mathbb{Z})$. Then $\xi = UA\xi$, consequently $UA \in \mathrm{Stab}(\xi) \setminus \mathrm{Stab}^+(\xi)$, and by Theorem 1.2.2 there exists some $(x, y) \in \mathbb{Z}^2$ such that $x^2 - \Delta y^2 = -4$.

(c) $\Rightarrow$ (a) Let $x, y \in \mathbb{Z}$ be such that $x^2 - \Delta y^2 = -4$, and let ξ_1, ξ_2 be two equivalent quadratic irrationals of discriminant Δ, say $\xi_2 = A\xi_1$, where $A \in \mathsf{GL}_2(\mathbb{Z})$. If $\det(A) = 1$, then ξ_1 and ξ_2 are properly equivalent. If $\det(A) = -1$, then Theorem 1.2.2 implies that there is some $B \in \mathrm{Stab}(\xi_2)$ such that $\det(B) = -1$, and since $\xi_2 = BA\xi_1$ and $\det(BA) = 1$, it follows again that ξ_1 and ξ_2 are properly equivalent. □

For a quadratic discriminant Δ, we denote by

- $\mathfrak{X}_\Delta$ the set of all equivalence classes of quadratic irrationals with discriminant Δ;
- $\mathfrak{X}_\Delta^+$ the set of all proper equivalence classes of quadratic irrationals with discriminant Δ.

Corollary 1.3.9. *Let Δ be a quadratic discriminant. If Pell's minus equation for Δ has integral solutions, then $\mathfrak{X}_\Delta = \mathfrak{X}_\Delta^+$. Otherwise every equivalence class $X \in \mathfrak{X}_\Delta$ splits into two disjoint proper equivalence classes X' and X'',*

$$X = X' \uplus X'', \quad \text{and} \quad X'' = \{-\xi \mid \xi \in X'\}.$$

Proof. By Theorem 1.3.8. □

Theorem and Definition 1.3.10 (Class numbers)**.** *Let* Δ *be a quadratic discriminant. Then there are only finitely many reduced quadratic irrationals of discriminant* Δ*. In particular, the sets* $\mathfrak{X}_\Delta$ *and* $\mathfrak{X}_\Delta^+$ *are finite.*

We set

$$h_\Delta = |\mathfrak{X}_\Delta| \quad \textit{and} \quad h_\Delta^+ = \begin{cases} h_\Delta & \textit{if} \quad \Delta < 0\,, \\ |\mathfrak{X}_\Delta^+| & \textit{if} \quad \Delta > 0\,. \end{cases}$$

We call h_Δ the *the class number* and h_Δ^+ the *the narrow class number* of discriminant Δ.

- *If* $\Delta < 0$*, then* h_Δ *is the number of reduced quadratic irrationals of discriminant* Δ*, and* $|\mathfrak{X}_\Delta^+| = 2h_\Delta$.
- *If* $\Delta > 0$*, then*

$$h_\Delta^+ = \begin{cases} h_\Delta & \textit{if Pell's minus equation for } \Delta \textit{ has integral solutions}\,, \\ 2h_\Delta & \textit{otherwise}\,. \end{cases}$$

Only in the later Chapters 5 and 6 it will become evident why, for $\Delta < 0$, we set $h_\Delta^+ = |\mathfrak{X}_\Delta|$ and not $h_\Delta^+ = |\mathfrak{X}_\Delta^+|$.

Proof. There are only finitely many pairs $(a,b) \in \mathbb{Z}^2$ such that

$$\begin{cases} 0 < a < \sqrt{|\Delta|/3} \quad \text{and} \quad |b| \le a & \text{if} \quad \Delta < 0\,, \\ 0 < a < \sqrt{\Delta} \quad \text{and} \quad 0 < b < \sqrt{\Delta} & \text{if} \quad \Delta > 0\,. \end{cases}$$

According to the Theorems 1.3.2 and 1.3.5, for each such pair $(a,b) \in \mathbb{Z}^2$ there is at most one reduced quadratic irrational of type (a,b,c) and discriminant $\Delta = b^2 - 4ac$. Hence the number of reduced quadratic irrationals of discriminant Δ is finite.

CASE 1 : $\Delta < 0$. By Theorem 1.3.2.1, every quadratic irrational of discriminant Δ is equivalent to precisely one reduced quadratic irrational. Hence $h_\Delta = |\mathfrak{X}_\Delta|$ is the number of reduced quadratic irrationals of discriminant Δ. In this case, Pell's minus equation has no integral solutions, and Corollary 1.3.9 implies $|\mathfrak{X}_\Delta^+| = 2|\mathfrak{X}_\Delta| = 2h_\Delta$.

CASE 2 : $\Delta > 0$. By Theorem 1.3.5, every quadratic irrational of discriminant Δ is properly equivalent to a reduced quadratic irrational. However, in general there are several such ξ_0, and we remind the reader of the fact that the proof of this assertions was postponed to Theorem 2.2.2. Since there are only finitely many reduced quadratic irrationals of discriminant Δ, it follows that $h_\Delta = |\mathfrak{X}_\Delta| < \infty$, and by Corollary 1.3.9 we obtain

$$h_\Delta^+ = |\mathfrak{X}_\Delta^+| = \begin{cases} h_\Delta & \text{if Pell's minus equation for } \Delta \text{ has integral solutions,} \\ 2h_\Delta & \text{otherwise}\,. \end{cases} \qquad \square$$

1.4. Two short tables of class numbers

We close this chapter with a short table of class numbers h_Δ for quadratic discriminants Δ for $|\Delta| \leq 500$. Of course, there exist larger tables, for example in Mollin's book [**74**], or in [**27**]. The tables below should encourage an ambitious reader to make his own numerical experiments and to do some examples by hand.

For $\Delta < 0$, h_Δ is the number of reduced forms of discriminant Δ by Theorem 1.3.10, and the entries of our table can be verified as in Example 1.3.3 or in Exercise 1.3.4.

For $\Delta > 0$, we shall derive the methods to reproduce the table only in Chapter 2. In this case, h_Δ is the number of equivalence classes of periods of discriminant Δ (see Remarks and Definition 2.2.3). Some cases are explicitly done in Example 2.2.10, but we also refer to the Exercises 1.3.7 and 2.1.15.

$$\Delta < 0$$

Δ	-3	-4	-7	-8	-11	-12	-15	-16	-19	-20	-23	-24	-27	-28	-31	-32
h_Δ	1	1	1	1	1	1	2	1	1	2	3	2	1	1	3	2

Δ	-35	-36	-39	-40	-43	-44	-47	-48	-51	-52	-55	-56	-59	-60	-63
h_Δ	2	2	4	2	1	3	5	2	2	2	4	4	3	2	4

Δ	-64	-67	-68	-71	-72	-75	-76	-79	-80	-83	-84	-87	-88	-91	-92
h_Δ	2	1	4	7	2	2	3	5	4	3	4	6	2	2	3

Δ	-95	-96	-99	-100	-103	-104	-107	-108	-111	-112	-115	-116
h_Δ	8	4	2	2	5	6	3	3	8	2	2	6

Δ	-119	-120	-123	-124	-127	-128	-131	-132	-135	-136	-139	-140
h_Δ	10	4	2	3	5	4	5	4	6	4	3	6

Δ	-143	-144	-147	-148	-151	-152	-155	-156	-159	-160	-163	-164
h_Δ	10	4	2	2	7	6	4	4	10	4	1	8

Δ	-167	-168	-171	-172	-175	-176	-179	-180	-183	-184	-187	-188
h_Δ	11	4	4	3	6	6	5	4	8	4	2	5

Δ	-191	-192	-195	-196	-199	-200	-203	-204	-207	-208	-211	-212
h_Δ	13	4	4	4	9	6	4	6	6	4	3	6

Δ	-215	-216	-219	-220	-223	-224	-227	-228	-231	-232	-235	-236
h_Δ	14	6	4	4	7	8	5	4	12	2	2	9

Δ	-239	-240	-243	-244	-247	-248	-251	-252	-255	-256	-259	-260
h_Δ	15	4	3	6	6	8	7	4	12	4	4	8

Δ	-263	-264	-267	-268	-271	-272	-275	-276	-279	-280	-283	-284
h_Δ	13	8	2	3	11	8	4	8	12	4	3	7

Δ	-287	-288	-291	-292	-295	-296	-299	-300	-303	-304	-307	-308
h_Δ	14	4	4	4	8	10	8	6	10	6	3	8

Δ	-311	-312	-315	-316	-319	-320	-323	-324	-327	-328	-331	-332
h_Δ	19	4	4	5	10	8	4	6	12	4	3	9

Δ	-335	-336	-339	-340	-343	-344	-347	-348	-351	-352	-355	-356
h_Δ	19	4	4	5	10	8	4	6	12	4	3	9

Δ	-359	-360	-363	-364	-367	-368	-371	-372	-375	-376	-379	-380
h_Δ	19	8	4	6	9	6	8	4	10	8	3	8

Δ	-383	-384	-387	-388	-391	-392	-395	-396	-399	-400	-403	-404
h_Δ	17	8	4	4	14	8	8	6	16	4	2	14

Δ	-407	-408	-411	-412	-415	-416	-419	-420	-423	-424	-427	-428
h_Δ	16	4	6	5	10	12	9	8	10	6	2	9

Δ	-431	-432	-435	-436	-439	-440	-443	-444	-447	-448	-451	-452
h_Δ	21	6	4	6	15	12	5	8	14	4	6	8

Δ	-455	-456	-459	-460	-463	-464	-467	-468	-471	-472	-475	-476
h_Δ	20	8	6	6	7	12	7	8	16	6	4	10

Δ	-479	-480	-483	-484	-487	-488	-491	-492	-495	-496	-499	-500
h_Δ	25	8	4	6	7	10	9	6	16	6	3	10

$\Delta > 0$

Δ	5*	8*	12	13*	17*	20*	21	24	28	29*	32	33	37*	40*	41*	44
h^+_Δ	1	1	2	1	1	1	2	2	2	1	2	2	1	2	1	2

Δ	45	48	52*	53*	56	57	60	61*	65*	68*	69	72	73*	76	77	80
h^+_Δ	2	2	1	1	2	2	4	1	2	1	2	2	1	2	2	2

Δ	84	85*	88	89*	92	93	96	97*	101*	104*	105	108	109*	112
h^+_Δ	2	2	2	1	2	2	4	1	1	2	4	2	1	2

Δ	113*	116*	117	120	124	125*	128	129	132	133	136	137*	140
h^+_Δ	1	1	2	4	2	1	2	2	2	2	4	1	4

Δ	141	145*	148*	149*	152	153*	156	157*	160	161	164*	165	168
h^+_Δ	2	4	3	1	2	2	4	1	4	2	1	4	4

Δ	172	173*	176	177	180	181*	184	185*	188	189	192	193*	197*
h^+_Δ	2	1	2	2	2	1	2	2	2	2	4	1	1

Δ	200*	201	204	205	208	209	212*	213	216	217	220	221	224
h^+_Δ	2	2	4	4	2	2	1	2	2	2	4	4	4

Δ	228	229*	232*	233*	236	237	240	241*	244*	245	248	249	252
h^+_Δ	2	3	2	1	2	2	4	1	1	2	2	2	4

Δ	253	257*	260*	261	264	265*	268	269*	272	273	276	277*	280
h^+_Δ	2	3	2	2	4	2	2	1	2	4	2	1	4

Δ	281	284	285	288	292*	293*	296*	297	300	301	304	305	308
h^+_Δ	1	2	4	4	1	1	2	2	4	2	2	4	2

Δ	309	312	313*	316	317*	320	321	325*	328*	329	332	333	336
h^+_Δ	2	4	1	6	1	4	6	2	4	2	2	2	4

Δ	337*	340*	341	344	345	348	349*	352	353*	356*	357	360	364
h^+_Δ	1	2	2	2	4	4	1	4	1	1	4	4	4

Δ	365*	368	369	372	373*	376	377	380	381	384	385	388*	389*
h^+_Δ	2	2	2	2	1	2	4	4	2	4	4	1	1

Δ	392	393	396	397*	401*	404*	405	408	409*	412	413	416	417
h^+_Δ	2	2	8	1	5	3	2	4	1	2	2	4	2

Δ	420	421	424*	425*	428	429	432	433*	436*	437	440	444	445*
h^+_Δ	4	1	2	2	2	4	2	1	1	2	4	4	4

Δ	448	449*	452*	453	456	457*	460	461*	464*	465	468	469	472
h^+_Δ	4	1	1	2	4	1	4	1	2	4	2	6	2

Δ	473	476	477	480	481*	485*	488*	489	492	493*	496	497	500*
h^+_Δ	6	4	2	8	2	2	2	2	4	2	2	2	1

This page intentionally left blank

CHAPTER 2

Continued fractions

The digit expansion of an irrational real number z produces rational approximations with arbitrary exactitude. If we use (say) g-adic digit expansions, we usually need a dominator of size $N = g^n$ to accomplish an approximation with an error less than $N^{-1} = g^{-n}$. In contrast, Dirichlet's approximation theorem shows that a suitable choice of denominator q gives rise to an approximation with an error less than q^{-2} (see Theorem 1.2.3). A systematic way to produce such good approximations with small denominators is provided by the theory of continued fractions, which is a main tool in the theory of Diophantine approximation.

In this volume however, Diophantine approximation plays only a minor role. Our main reason for a detailed study of continued fractions lies in the fact that the continued fraction of a real quadratic irrational z is ultimately periodic, and that the period carries arithmetical information about z. We shall derive the general theory as far as it is needed for our purpose in Section 2.1, and then we shall concentrate on the theory of real quadratic irrationals. In Section 2.2 we prove the classical periodicity results of Euler, Lagrange and Galois, and we provide a detailed study of the solutions of Pell's equation, a topic whose importance was already mentioned in Chapter 1 (see Theorem 1.3.8 and the comments preceding Theorem 1.2.3). In Section 2.3 we introduce ambiguous and symmetric quadratic irrationals and their continued fractions. These concepts will prove to be the appropriate tool for the investigation of the ideal class groups of real quadratic orders in Chapter 5.

The basics of the theory of continued fractions are contained in almost every book on elementary number theory. Our main reference is the classical book of O. Perron [**90**]. Other valuable sources are [**70**] and [**43**]. A wealth of details and numerical examples can be found R. A. Mollin's book [**74**]. Concerning Pell's equation, we also refer to [**42**, §16].

2.1. General theory of continued fractions

For a (finite or infinite) sequence $(u_n)_{n\geq 0}$ in $\mathbb{R}$ such that $u_n > 0$ for all $n \geq 1$, we define the *continued fractions* $[u_0, u_1, \ldots, u_n]$ for $n \geq 0$ recursively by

$$[u_0] = u_0\,, \quad \text{and} \quad [u_0, \ldots, u_{n-1}, u_n] = \Big[u_0, \ldots, u_{n-2}, u_{n-1} + \frac{1}{u_n}\Big] \quad \text{for} \quad n \geq 1\,.$$

Explicitly, we obtain

$$[u_0,u_1]=u_0+\frac{1}{u_1}\,,\quad \text{and}\quad [u_0,u_1,\ldots,u_n]\;=\;u_0+\cfrac{1}{u_1+\cfrac{1}{u_2+\cfrac{1}{\ddots\;+\cfrac{1}{u_{n-1}+\cfrac{1}{u_n}}}}}$$

for all $n\ge 1$. In particular, it follows that $[u_0,u_1,\ldots,u_n]\in\mathbb{R}$ for all $n\ge 0$.

Connected with the sequence $(u_n)_{n\ge0}$, we define recursively two (again finite or infinite) sequences $(p_n)_{n\ge-2}$ and $(q_n)_{n\ge-2}$ by

$$\begin{aligned} &p_{-2}=0\,,\quad p_{-1}=1\,,\quad \text{and}\quad p_n=u_np_{n-1}+p_{n-2}\quad\text{for all}\ \ n\ge0\,,\\ &q_{-2}=1\,,\quad q_{-1}=0\,,\quad \text{and}\quad q_n=u_nq_{n-1}+q_{n-2}\quad\text{for all}\ \ n\ge0\,. \end{aligned}\tag{1}$$

Then $p_0=u_0$, $p_1=u_0u_1+1$, $q_0=q_{-2}=1$ and $q_1=u_1q_0=u_1>0$. By an easy induction we obtain $q_n>0$ for all $n\ge0$, and thus $q_n>q_{n-2}>0$ for all $n\ge2$.

It is convenient to write (1) in matrix form. Then

$$\begin{pmatrix}p_{-1}&p_{-2}\\q_{-1}&q_{-2}\end{pmatrix}=\begin{pmatrix}1&0\\0&1\end{pmatrix}\quad\text{and}\quad\begin{pmatrix}p_n&p_{n-1}\\q_n&q_{n-1}\end{pmatrix}=\begin{pmatrix}u_n&1\\1&0\end{pmatrix}\begin{pmatrix}p_{n-1}&p_{n-2}\\q_{n-1}&q_{n-2}\end{pmatrix}\quad\text{for}\ \ n\ge0\,.$$

By induction it follows that, for all $n\ge-1$,

$$\begin{pmatrix}p_n&p_{n-1}\\q_n&q_{n-1}\end{pmatrix}=\prod_{i=0}^{n}\begin{pmatrix}u_i&1\\1&0\end{pmatrix}\quad\text{and}\quad\det\begin{pmatrix}p_n&p_{n-1}\\q_n&q_{n-1}\end{pmatrix}=p_nq_{n-1}-p_{n-1}q_n=(-1)^{n+1}\,.$$

Theorem 2.1.1. *Let $(u_n)_{n\ge0}$ be a (finite or infinite) sequence in $\mathbb{R}$ such that $u_n>0$ for all $n\ge1$, and let the sequences $(p_n)_{n\ge-2}$ and $(q_n)_{n\ge-2}$ be defined by* (1).

1. *If $0\le m<n$, then $\big[u_0,\ldots,u_m,[u_{m+1},\ldots,u_n]\big]=[u_0,u_1,\ldots,u_n]$.*
2. *If $n\ge0$ and $x\in\mathbb{R}_{>0}$, then*

$$[u_0,u_1,\ldots,u_{n-1},x]=\frac{p_{n-1}x+p_{n-2}}{q_{n-1}x+q_{n-2}}\,,\qquad\textit{and}$$
$$[u_0,u_1,\ldots,u_n]=\frac{p_n}{q_n}\,.$$

3. *If $x\in\mathbb{R}_{>0}$, then $u_0<[u_0,x]=u_0+x^{-1}$, and*

$$u_0<[u_0,u_1,\ldots,u_{n-1},x]<u_0+\frac{1}{u_1}\quad\textit{for all}\ \ n\ge2\,.$$

4. *If $n\ge0$ and $u_i\in\mathbb{Z}$ for all $i\in[0,n]$, then it follows that $p_n\in\mathbb{Z}$, $q_n\in\mathbb{N}$,*

$$[u_0,\ldots,u_n]\in\mathbb{Q}\quad\textit{and}\quad(p_n,p_{n-1})=(q_n,q_{n-1})=(p_n,q_n)=1\,.$$

In particular, p_n is the reduced numerator and q_n is the reduced denominator of $[u_0,\ldots,u_n]$.

PROOF. 1. Let $m \geq 0$ be fixed, and use induction on $n \geq m+1$. For $n = m+1$ there is nothing to do.

$n > m+1\,,\ n-1 \to n:$ By definition and the induction hypothesis we obtain

$$[u_0, \ldots, u_m, [u_{m+1}, \ldots, u_{n-1}, u_n]] = \Big[u_0, \ldots, u_m, \Big[u_{m+1}, \ldots, u_{n-2}, u_{n-1} + \frac{1}{u_n}\Big]\Big]$$
$$= \Big[u_0, \ldots, u_{n-2}, u_{n-1} + \frac{1}{u_n}\Big] = [u_0, \ldots, u_{n-1}, u_n]\,.$$

2. We use induction on n. For $n = 0$, the assertion is obvious.

$n \geq 1\,,\ n-1 \to n:$ By definition and the induction hypothesis we obtain

$$[u_0, u_1, \ldots, u_{n-1}, x] = \Big[u_0, \ldots, u_{n-2}, u_{n-1} + \frac{1}{x}\Big]$$
$$= \frac{\Big(u_{n-1} + \dfrac{1}{x}\Big) p_{n-2} + p_{n-3}}{\Big(u_{n-1} + \dfrac{1}{x}\Big) q_{n-2} + q_{n-3}}$$
$$= \frac{p_{n-1} + \dfrac{p_{n-2}}{x}}{q_{n-1} + \dfrac{q_{n-2}}{x}} = \frac{p_{n-1}x + p_{n-2}}{q_{n-1}x + q_{n-2}} \qquad \Big[= \frac{p_n}{q_n} \ \text{ if } \ x = u_n\Big].$$

3. We obviously have $u_0 + x^{-1} = [u_0, x] > u_0$. If $n \geq 2$, then 1. implies $u_1 < \big[u_1, [u_2, \ldots, u_{n-1}, x]\big] = [u_1, \ldots, u_{n-1}, x]$ and

$$u_0 < [u_0, \ldots, u_{n-1}, x] = \big[u_0, [u_1, \ldots, u_{n-1}, x]\big]$$
$$= u_0 + \frac{1}{[u_1, \ldots, u_{n-1}, x]} < u_0 + \frac{1}{u_1}\,.$$

4. By induction on n it follows that $p_n \in \mathbb{Z},\ q_n \in \mathbb{N}$ and $[u_0, u_1, \ldots, u_n] \in \mathbb{Q}$, and since $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1}$, we get $(p_n, p_{n-1}) = (q_n, q_{n-1}) = (p_n, q_n) = 1$. $\square$

Our next theorem paves the way for the investigation of infinite continued fractions, the representation of real number by means of continued fractions and the announced approximation properties.

Theorem 2.1.2. *Let $(u_n)_{n \geq 0}$ be a sequence of real numbers such that $u_n \geq 1$ for all $n \geq 1$, and let the sequences $(p_n)_{n \geq -2}$ and $(q_n)_{n \geq -2}$ be defined as in* (1).

1. *If $n \geq 0$, then $0 \leq q_{n-1} \leq q_n$, and if $n \geq 2$, then even $q_n \geq q_{n-1} + 1 \geq n$.*
2. *If $u_0 \geq 0$, then $u_0 = p_0 < p_1 \leq p_2$, $\ p_n > p_{n-1}$ for all $n \geq 3$, and if $u_0 > 0$, then $p_1 < p_2$.*
3. *If $n \geq 2$, then*

$$\frac{p_{n-2}}{q_{n-2}} < \frac{p_n}{q_n} \ \ \textit{if} \ \ n \equiv 0 \bmod 2\,, \qquad \frac{p_{n-2}}{q_{n-2}} > \frac{p_n}{q_n} \ \ \textit{if} \ \ n \equiv 1 \bmod 2\,,$$

and

$$\Big(\Big[\frac{p_{2n}}{q_{2n}}, \frac{p_{2n+1}}{q_{2n+1}}\Big]\Big)_{n \geq 0} \quad \textit{is a sequence of nested intervals.}$$

4. *If* $n \geq 1$, *then*

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{(-1)^{n+1}}{q_{n-1}q_n}\,, \quad z = \lim_{n\to\infty} \frac{p_n}{q_n} \ \text{exists in } \mathbb{R}\,,$$

$$u_0 = \lfloor z \rfloor < z < u_0 + \frac{1}{u_1} \leq u_0 + 1\,,$$

and if $m \geq 0$, *then*

$$z = \lim_{n\to\infty} [u_0, \ldots, u_n] = \bigl[u_0, \ldots, u_m, \lim_{n\to\infty} [u_{m+1}, \ldots u_n]\bigr]\,.$$

Proof. 1. We use induction on n.

$n \leq 2$: $q_{-1} = 0$, $q_0 = 1$, $q_1 = u_1 \geq 1$ and $q_2 = u_1 q_1 + q_0 \geq u_1 + 1 \geq 2$.

$n \geq 3$, $n-1 \to n$: Suppose that $q_{n-1} \geq q_{n-2} + 1 \geq n-1$. Then it follows that $q_{n-2} \geq n-2 \geq 1$ and therefore $q_n = u_n q_{n-1} + q_{n-2} \geq q_{n-1} + q_{n-2} \geq q_{n-1} + 1 \geq n$.

2. Again, we use induction on n.

$n \in \{1, 2\}$: $p_1 = u_0 u_1 + 1 > u_0 = p_0 \geq 0$, hence $p_2 = u_2 p_1 + p_0 \geq p_1 + u_0 \geq p_1$, and $p_2 > p_1$ if $u_0 > 0$.

$n \geq 3$, $n-1 \to n$: If $p_{n-1} \geq p_{n-2} > 0$, then $p_n = u_n p_{n-1} + p_{n-2} > p_{n-1}$.

3. and 4. If $n \geq 1$, then

$$\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}} = \frac{p_n q_{n-1} - p_{n-1} q_n}{q_n q_{n-1}} = \frac{(-1)^{n+1}}{q_n q_{n-1}} \begin{cases} > 0 & \text{if } n \text{ is odd,} \\ < 0 & \text{if } n \text{ is even}\,. \end{cases}$$

For $n \geq 2$ this implies

$$\begin{aligned} \frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} &= \Bigl(\frac{p_n}{q_n} - \frac{p_{n-1}}{q_{n-1}}\Bigr) + \Bigl(\frac{p_{n-1}}{q_{n-1}} - \frac{p_{n-2}}{q_{n-2}}\Bigr) = \frac{(-1)^{n+1}}{q_n q_{n-1}} + \frac{(-1)^n}{q_{n-1} q_{n-2}} \\ &= \frac{(-1)^n}{q_{n-1}} \Bigl(\frac{1}{q_{n-2}} - \frac{1}{q_n}\Bigr), \quad \text{and thus} \quad \operatorname{sgn}\Bigl(\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}}\Bigr) = (-1)^n\,, \end{aligned}$$

since $q_n > q_{n-2}$. Hence

$$\Bigl(\Bigl[\frac{p_{2n}}{q_{2n}}, \frac{p_{2n+1}}{q_{2n+1}}\Bigr]\Bigr)_{n\geq 0}$$

is a sequence of nested intervals, and therefore the sequence

$$\Bigl(\frac{p_n}{q_n}\Bigr)_{n\geq 0} = \bigl([u_0, u_1, \ldots, u_n]\bigr)_{n\geq 0} \quad \text{converges.}$$

If $m \in \mathbb{N}_0$, then $x \mapsto [u_0, \ldots, u_m, x]$ is a rational function in $x \in \mathbb{R}_{>0}$. It is continuous, and therefore

$$\begin{aligned} z = \lim_{n\to\infty} \frac{p_n}{q_n} &= \lim_{n\to\infty} [u_0, \ldots, u_m, u_{m+1}, \ldots, u_n] \\ &= \lim_{n\to\infty} \bigl[u_0, \ldots, u_m, [u_{m+1}, \ldots, u_n]\bigr] \\ &= \bigl[u_0, \ldots, u_m, \lim_{n\to\infty} [u_{m+1}, \ldots, u_n]\bigr]\,. \end{aligned}$$

In particular,

$$\text{if} \quad x = \lim_{n\to\infty} [u_2, \ldots, u_n]\,, \quad \text{then} \quad z = [u_0, u_1, x]\,,$$

and

$$u_0 = \lfloor z \rfloor < z < u_0 + \frac{1}{u_1} \leq u_0 + 1 \quad \text{by Theorem 2.1.1.3.}$$

□

If $z \in \mathbb{Q}$ and $z = [u_0, u_1, \ldots, u_n]$, where $n \in \mathbb{N}_0$, $u_0 \in \mathbb{Z}$ and $u_1, \ldots, u_n \in \mathbb{N}$, then (by abuse of language) this representation (rather than the sequence $(u_0, \ldots, u_n)$) is called a (*finite*) *continued fraction* of z. If p_i and q_i for $i \in [-2, n]$ are defined by (1), then $p_i \in \mathbb{Z}$ and $q_i \in \mathbb{N}$ for all $i \in [0, n]$ by Theorem 2.1.1.4, and we call p_i the *i-th partial numerator*, q_i the *i-th partial denominator* and $\frac{p_i}{q_i}$ the *i-th convergent* of this continued fraction.

If $z \in \mathbb{R}$, $u_0 \in \mathbb{Z}$ and $(u_n)_{n\geq 0}$ is a sequence in $\mathbb{N}$ such that

$$z = \lim_{n\to\infty} [u_0, u_1, \ldots, u_n]\,, \quad \text{then we write} \quad z = [u_0, u_1, \ldots]\,,$$

and (again by abuse of language) we call this representation (rather than the sequence $(u_n)_{n\geq 0}$) the (*infinite*) *continued fraction* of z. In the subsequent Theorem 2.1.3 we shall prove that the continued fraction of a rational number is always finite (but not unique), and that every irrational number has a unique (infinite) continued fraction.

Consequently, if $z = [u_0, u_1, \ldots] \in \mathbb{R} \setminus \mathbb{Q}$, then it follows that the sequences $(p_n)_{n\geq -2}$ and $(q_n)_{n\geq -2}$ defined in (1) and the numbers $z_n = [u_n, u_{n+1}, \ldots] \in \mathbb{R} \setminus \mathbb{Q}$ (for $n \geq 0$) are uniquely determined by z. We call p_n the *n-th partial numerator*, q_n the *n-th partial denominator*, $\frac{p_n}{q_n}$ the *n-th convergent* and z_n the *n-th complete quotient* of z. Again, it follows that $p_n \in \mathbb{Z}$ and $q_n \in \mathbb{N}$ for all $n \geq 0$.

Theorem 2.1.3 (Existence and uniqueness of continued fractions)**.** *Let z be a real number.*

1. *If $z \in \mathbb{Q}$, then z has precisely two continued fractions. They are finite and of the form $z = [u_0, u_1, \ldots, u_k] = [u_0, \ldots, u_{k-1}, u_k - 1, 1]$, where $u_0 \in \mathbb{Z}$, and either $k = 0$, or $k \in \mathbb{N}$, $u_1, \ldots, u_k \in \mathbb{N}$ and $u_k \geq 2$. In particular, z has precisely one continued fraction whose length has a preassigned parity.*
2. *If $z \in \mathbb{R}\setminus\mathbb{Q}$, then z has a unique (infinite) continued fraction $z = [u_0, u_1, \ldots]$. Let $(p_n)_{n\geq -2}$ be the sequence of partial numerators, $(q_n)_{n\geq -2}$ the sequence of partial denominators and $(z_n)_{n\geq 0}$ the sequence of complete quotients of z. Then the following assertions hold for all $n \geq 0$:*

$$u_n = \lfloor z_n \rfloor\,, \quad z_{n+1} = z_n^{\#} = \frac{1}{z_n - \lfloor z_n \rfloor} \quad \textit{is the successor of } z,$$

$$z - \frac{p_n}{q_n} \;=\; \frac{(-1)^n}{q_n(q_n z_{n+1} + q_{n-1})}$$

and

$$\frac{1}{q_n(q_n + q_{n+1})} \;<\; \Bigl| z - \frac{p_n}{q_n} \Bigr| \;<\; \frac{1}{q_n q_{n+1}} \;\leq\; \frac{1}{q_n^2}\,.$$

PROOF. *Existence*:

CASE 1: $z \in \mathbb{Z}$. We set $u_0 = z$ and obtain $z = [u_0] = [u_0 - 1, 1]$.

CASE 2: $z \in \mathbb{Q} \setminus \mathbb{Z}$. Suppose that

$$z = \frac{p}{q}\,, \quad \text{where} \quad p \in \mathbb{Z}\,,\ q \in \mathbb{N} \ \text{ and } q \nmid p\,.$$

By the Euclidean algorithm, we obtain the following sequence of $k+1$ divisions with remainder (for some $k \in \mathbb{N}$):

$$\begin{aligned}
r_{-1} = p &= u_0 q + r_1\,, &&\text{where}\quad u_0 \in \mathbb{Z}\,,\ r_1 \in [1, q-1]\,,\\
r_0 = q &= u_1 r_1 + r_2\,, &&\text{where}\quad u_1 \in \mathbb{N}\,,\ r_2 \in [1, r_1-1]\,,\\
r_1 &= u_2 r_2 + r_3\,, &&\text{where}\quad u_2 \in \mathbb{N}\,,\ r_3 \in [1, r_2-1]\,,\\
&\ \ \vdots\\
r_{k-2} &= u_{k-1} r_{k-1} + r_k\,, &&\text{where}\quad u_{k-1} \in \mathbb{N}\,,\ r_k \in [1, r_{k-1}-1]\,,\\
r_{k-1} &= u_k r_k\,, &&\text{where}\quad u_k \in \mathbb{N}\,,\ u_k \geq 2\,.
\end{aligned}$$

Now we prove by induction on i that

$$\frac{p}{q} = \Bigl[u_0, \ldots, u_i, \frac{r_i}{r_{i+1}}\Bigr] \quad \text{for all} \quad i \in [-1, k-1]\,.$$

Finally, for $i = k-1$ this implies

$$\frac{p}{q} = [u_0, u_1, \ldots, u_k] = [u_0, u_1, \ldots, u_{k-1}, u_k - 1, 1]\,.$$

For $i = -1$ there is nothing to do, since $r_{-1} = p$ and $r_0 = q$.

$i \in [0, k-1]\,,\ i-1 \to i$: Using the induction hypothesis, we obtain

$$\begin{aligned}
\frac{p}{q} = \Bigl[u_0, \ldots, u_{i-1}, \frac{r_{i-1}}{r_i}\Bigr] &= \Bigl[u_0, \ldots, u_{i-1}, \frac{u_i r_i + r_{i+1}}{r_i}\Bigr]\\
&= \Bigl[u_0, \ldots, u_{i-1}, u_i + \frac{r_{i+1}}{r_i}\Bigr] = \Bigl[u_0, \ldots, u_i, \frac{r_i}{r_{i+1}}\Bigr]\,.
\end{aligned}$$

CASE 3: $z \in \mathbb{R} \setminus \mathbb{Q}$. We define sequences $(u_n)_{n\geq 0}$ in $\mathbb{Z}$ and $(z_n)_{n\geq 0}$ in $\mathbb{R} \setminus \mathbb{Q}$ recursively by $z_0 = z$, $u_n = \lfloor z_n \rfloor$, and

$$z_{n+1} = z_n^{\#} = \frac{1}{z_n - \lfloor z_n \rfloor} \quad \text{for} \quad n \geq 0\,.$$

If follows by the very definition that $z_n > 1$ and $u_n \in \mathbb{N}$ for all $n \geq 1$. We show by induction on n, that $z = [u_0, \ldots, u_n, z_{n+1}]$ for all $n \geq -1$.

For $n = -1$, this is obvious.

$n \geq 0\,,\ n-1 \to n$: If $n \geq 0$ and $z = [u_0, \ldots, u_{n-1}, z_n]$, then

$$z = [u_0, \ldots, u_{n-1}, z_n] = \Bigl[u_0, \ldots, u_{n-1}, u_n + \frac{1}{z_{n+1}}\Bigr] = [u_0, \ldots, u_n, z_{n+1}]\,.$$

Let $(p_n)_{n\geq -2}$ and $(q_n)_{n\geq -2}$ be defined by (1). Then

$$[u_0, u_1, \ldots] = \lim_{n\to\infty} \frac{p_n}{q_n}\,, \quad \text{and thus we must prove that} \quad z = \lim_{n\to\infty} \frac{p_n}{q_n}\,.$$

If $n \in \mathbb{N}_0$, then $z = [u_0, \ldots, u_n, z_{n+1}]$, and Theorem 2.1.1.2 implies

$$z - \frac{p_n}{q_n} = \frac{p_n z_{n+1} + p_{n-1}}{q_n z_{n+1} + q_{n-1}} - \frac{p_n}{q_n} = \frac{p_{n-1} q_n - p_n q_{n-1}}{q_n(q_n z_{n+1} + q_{n-1})} = \frac{(-1)^n}{q_n(q_n z_{n+1} + q_{n-1})}\,.$$

By Theorem 2.1.2 we obtain $u_{n+1} < z_{n+1} = [u_{n+1}, z_{n+2}] < u_{n+1} + 1$, and

$$n \leq q_n \leq q_{n+1} = q_n u_{n+1} + q_{n-1} < q_n z_{n+1} + q_{n-1} < q_n u_{n+1} + q_n + q_{n-1} = q_n + q_{n+1}\,.$$

Hence it follows that

$$\frac{1}{q_n(q_n+q_{n+1})} < \frac{1}{q_n(q_nz_{n+1}+q_{n-1})} = \Bigl|z-\frac{p_n}{q_n}\Bigr| < \frac{1}{q_nq_{n+1}} \le \frac{1}{q_n^2} \le \frac{1}{n^2}\,,$$

and, in particular, this implies convergence.

Uniqueness: We shall prove the following assertion:

A. Let $u_0,\,u_0'\in\mathbb{Z}$, $m,n\in\mathbb{N}_0$, $n\le m$, $u_1,\ldots,u_n,\,u_1',\ldots,u_m'\in\mathbb{N}$ and $x,\,x'\in\mathbb{R}_{\ge1}$ such that $[u_0,u_1,\ldots,u_n,x]=[u_0',u_1',\ldots,u_m',x']$. Then $u_i=u_i'$ for all $i\in[0,n]$, and $x=[u_{n+1}',\ldots,u_m',x']$.

We first prove the uniqueness using **A** in the following three steps:

I. If z has two finite continued fractions, then they are as asserted;
II. z cannot have both a finite and an infinite continued fraction;
III. if z has two infinite continued fractions, then they coincide.

I. Suppose that $z=[u_0,\,u_1,\ldots,u_k]=[u_0',\,u_1',\ldots,u_l']$, where $k,\,l\in\mathbb{N}_0$, $k\le l$, $u_0,\,u_0'\in\mathbb{Z}$ and $u_1,\ldots,u_k,\,u_1',\ldots,u_l'\in\mathbb{N}$.

CASE 1: $k=0$. Then $z=u_0=[u_0',u_1',\ldots,u_l']$. If $l=0$, then $u_0=u_0'$. If $l=1$, then $u_0=u_0'+u_1'^{-1}$, and since $u_1'\ge1$ it follows that $u_1'=1$ and $u_0'=u_0-1$. If $l\ge2$, then $u_0'<u_0<u_0'+u_1'^{-1}\le u_0'+1$, which is impossible.

CASE 2: $k\ge1$. Then $[u_0,\ldots,u_{k-1},\,u_k]=\bigl[u_0',\ldots,u_{k-1}',[u_k',\ldots,u_l']\bigr]$, and by **A** it follows that $u_i=u_i'$ for all $i\in[0,k-1]$ and $u_k=[u_k',\ldots,u_l']$. Since $u_k=[u_k]$, CASE 1 implies that either $k=l$, $u_k=u_k'$ or $l=k+1$, $u_k'=u_k-1$ and $u_{k+1}'=1$.

II. Assume to the contrary that z has a finite and an infinite continued fraction, say $z=[u_0,u_1,\ldots,u_k]=[u_0',u_1',\ldots]=[u_0',\ldots,u_{k-1}',[u_k',\,u_{k+1}',\ldots]]$, where $k\in\mathbb{N}_0$, $u_0,\,u_0'\in\mathbb{Z}$, $u_1,\ldots,u_k\in\mathbb{N}$ and $u_i'\in\mathbb{N}$ for all $i\ge1$. By **A**, it follows that $u_k=[u_k',\,u_{k+1}',\ldots]\in\mathbb{N}$, and thus $u_k'<u_k<u_k'+1$, a contradiction.

III. Suppose that $z=[u_0,u_1,\ldots]=[u_0',u_1',\ldots]$, where $u_0,\,u_0'\in\mathbb{Z}$ and $u_i,\,u_i'\in\mathbb{N}$ for all $i\ge1$. For $n\in\mathbb{N}$, we have $[u_0,\ldots,u_n,[u_{n+1},\ldots]]=[u_0',\ldots,u_n',[u_{n+1}',\ldots]]$, hence $u_i=u_i'$ for all $i\in[0,n]$ by **A**, and therefore it follows that $u_n=u_n'$ for all $n\ge0$.

Proof of **A**. We proceed by induction on n.

$n=0$: Since $[u_0,x]=[u_0',\ldots,u_m',\,x']=[u_0',[u_1',\ldots,u_m',\,x']]$, we obtain

$$u_0+\frac{1}{x}=u_0'+\frac{1}{[u_1',\ldots,u_m',x']}\,.$$

If $[u_1',\ldots,u_m',x']=1$, then $m=0$ and $x'=1$, hence $x=1$ and $u_0=u_0'$. If $[u_1',\ldots,u_m',x']>1$, then $x>1$, hence again $u_0=u_0'$ and $x=[u_1',\ldots,u_m',x']$.

$n\ge1$, $n-1\to n$: Since $[u_0,[u_1,\ldots,u_n,x]]=[u_0',[u_1',\ldots,u_m',x]]$, we obtain

$$u_0+\frac{1}{[u_1,\ldots,u_n,x]}=u_0'+\frac{1}{[u_1',\ldots,u_m',x']}\,.$$

As $[u_1,\ldots,u_n,x]>u_1\ge1$ and $[u_1',\ldots,u_m',x']\ge u_1'>1$, we get $u_0=u_0'$, $[u_1,\ldots,u_n,x]=[u_1',\ldots,u_m',x]$, and the assertion follows by the induction hypothesis. □

Exercise 2.1.4. Calculate the continued fractions of 0, $-\frac{82}{17}$ and $\frac{13}{100}$.

Exercise 2.1.5. Suppose that $b \in \mathbb{N}$. Prove that the reduced quadratic irrational $\theta_b = (b + \sqrt{b^2+4})/2$ has the periodic continued fraction $\theta_b = [b, b, b, \ldots]$, and that the partial denominators are given by

$$q_n = \frac{\theta_b^n - \theta_b^{-n}}{\sqrt{b^2+4}} \quad \text{for all } n \geq 0.$$

Consider in particular the case $b = 1$.

The Fibonacci sequence $(F_n)_{n \geq 0}$ is recursively defined by $F_0 = 0$, $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for all $n \geq 2$. Prove that

$$F_n = \frac{1}{2^{m-1}} \sum_{j=0}^{\infty} \binom{m}{2j+1} 5^j \quad \text{for all} \quad n \geq 1\,,$$

and

$$\frac{F_{n+1}}{F_n} \quad \text{is the } n\text{-th convergent of the golden ratio } \theta_1 = \frac{1+\sqrt{5}}{2}\,.$$

Exercise 2.1.6. Assume that $\pi = 3.1415926\ldots$ (correct to seven decimals). Prove that $\pi = [3, 7, 15, 1, \ldots]$, and the first three convergents of π are $\frac{22}{7}$, $\frac{333}{106}$ and $\frac{355}{113}$. Verify that $\left|\pi - \frac{355}{113}\right| < 10^{-6}$.

We continue with an application of continued fractions to the representation of a positive integer as a sum of two integral squares. In particular, we shall prove the classical result of Fermat that every prime $p \equiv 1 \bmod 4$ is a sum of two integral squares, and our proof will even provide an algorithm to produce these squares. We shall come back to this question at several places of this volume with different methods (see Section 3.4 and the Theorems 3.2.5, 6.2.6 and 6.2.13). Constructive proofs of Fermat's theorem by means of continued fractions or the Euclidean algorithm have a long history, and we refer to [**25**] for a thorough discussion. Our approach follows the version given in [**9**].

Theorem 2.1.7. *Let p and q be positive integers, $p > q$ and*

$$\frac{p}{q} = [u_0, u_1, \ldots, u_n]\,, \quad \textit{where } n \in \mathbb{N}_0 \textit{ and } u_0, \ldots, u_n \in \mathbb{N}\,.$$

Let $(p_i)_{i \in [-2,n]}$ be the sequence of partial numerators and $(q_i)_{i \in [-2,n]}$ the sequence of partial denominators of this continued fraction.

1. *We have*
$$[u_n, u_{n-1}, \ldots, u_0] = \frac{p_n}{p_{n-1}}\,.$$
2. *Suppose that $p \,|\, q^2+1$ and $n = 2k+1$ for some $k \in \mathbb{N}_0$. Then $p = p_k^2 + p_{k-1}^2$.*
3. *Every prime $p \equiv 1 \bmod 4$ is the sum of two integral squares.*

PROOF. 1. Induction on n.
$n = 0\colon\ p_{-1} = 1$ and $p_0 = u_0$.
$n \ge 1,\ n-1 \to n\colon$ By the induction hypothesis, we obtain

$$\begin{aligned}[u_n, u_{n-1}, \ldots, u_0] &= \big[u_n, [u_{n-1}, \ldots, u_0]\big] = u_n + \frac{1}{[u_{n-1}, \ldots, u_0]} \\ &= u_n + \frac{p_{n-2}}{p_{n-1}} = \frac{u_n p_{n-1} + p_{n-2}}{p_{n-1}} = \frac{p_n}{p_{n-1}}\,.\end{aligned}$$

2. By assumption, $(p,q) = 1$, hence $p = p_n,\ \ q = q_n,\ \ p_n > q_n$ and $q_n^2 + 1 = p_n b$ for some $b \in \mathbb{N}$. Since $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1} = 1$, we obtain

$$q_n(q_n - p_{n-1}) = (q_n^2 + 1) - (q_n p_{n-1} + 1) = p_n b - p_n q_{n-1} = p_n(b - q_{n+1})\,,$$

and since $(p_n, q_n) = 1$, it follows that $p_n \,|\, q_n - p_{n-1}$. The inequalities $p_n > q_n > 0$ and $p_n = u_n p_{n-1} + p_{n-2} > p_{n-1} > 0$ imply $p_n > q_n - p_{n-1}$ and $p_n > p_{n-1} - q_n$, hence $|p_{n-1} - q_n| < p_n$, and therefore $p_{n-1} = q_n$. Since

$$[u_0, u_1, \ldots, u_n] = \frac{p_n}{q_n} = \frac{p_n}{p_{n-1}} = [u_n, u_{n-1}, \ldots, u_0]\,,$$

the uniqueness in Theorem 2.1.3.1 implies $u_j = u_{n-j}$ for all $j \in [0,n]$, and therefore $u_{k+j} = u_{k+1-j}$ for all $j \in [0,k]$. Hence we obtain

$$\begin{aligned}\begin{pmatrix} p & p_{n-1} \\ q & q_{n-1}\end{pmatrix} &= \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1}\end{pmatrix} = \prod_{i=0}^{k} \begin{pmatrix} u_i & 1 \\ 1 & 0\end{pmatrix} = \prod_{i=0}^{k} \begin{pmatrix} u_i & 1 \\ 1 & 0\end{pmatrix} \prod_{i=0}^{k} \begin{pmatrix} u_{k-i} & 1 \\ 1 & 0\end{pmatrix} \\ &= \prod_{i=0}^{k} \begin{pmatrix} u_i & 1 \\ 1 & 0\end{pmatrix} \left[\prod_{i=0}^{k} \begin{pmatrix} u_i & 1 \\ 1 & 0\end{pmatrix}\right]^{\mathsf{t}} = \begin{pmatrix} p_k & p_{k-1} \\ q_k & q_{k-1}\end{pmatrix} \begin{pmatrix} p_k & q_k \\ p_{k-1} & q_{l-1}\end{pmatrix},\end{aligned}$$

and consequently $p = p_k^2 + p_{k-1}^2$.

3. Let $p \equiv 1 \bmod 4$ be a prime. By Theorem A.6.3.6, there exists some $x \in \mathbb{Z}$ such that $x^2 \equiv -1 \bmod p$, and we may assume that $0 < x < p$. Then $p \,|\, x^2 + 1$, and there is a continued fraction of even length

$$\frac{p}{x} = [u_0, u_1, \ldots, u_{2k+1}] \quad \text{for some } k \in \mathbb{N}_0.$$

Hence p is the sum of two integral squares by 2. □

Exercise 2.1.8. Write 10 006 721 as a sum of two squares.

Exercise 2.1.9. Let $(u_n)_{n\ge0}$ be a sequence in $\mathbb{R}$ such that $u_n > 0$ for all $n \ge 1$, and let the sequences $(p_n)_{n\ge-2}$ and $(q_n)_{n\ge-2}$ be defined as in (1).

a) Prove that $p_n q_{n-2} - p_{n-2} q_n = (-1)^n u_n$ for all $n \ge 0$,

$$[u_n, u_{n-1}, \ldots, u_0] = \frac{p_n}{p_{n-1}} \quad \text{for all } \ n \ge 0 \ \text{ if } \ u_0 > 0\,,$$

and

$$[u_n, u_{n-1}, \ldots, u_1] = \frac{q_n}{q_{n-1}} \quad \text{for all } \ n \ge 1\,.$$

b) Suppose that $n \ge 1$, $u_0, \ldots, u_n \in \mathbb{N}$, and $u_j = u_{n-j}$ for all $j \in [0, n]$. Then p_n divides $q_n^2 + (-1)^{n+1}$.

If $z \in \mathbb{R} \setminus \mathbb{Q}$, then we have proved in Theorem 1.2.3 (Dirichlet's approximation theorem) that there are infinitely many pairs $(p, q) \in \mathbb{Z} \times \mathbb{N}$ such that

$$\Bigl| z - \frac{p}{q} \Bigr| < \frac{1}{q^2},$$

and in Theorem 2.1.3.2 we have seen that the convergents of z have this property. In the subsequent Theorem 2.1.10 we shall, conversely, characterize the convergents of z by an approximation property. In Corollary 2.1.11 we use this result to derive a simple criterion for an approximating fraction to be a convergent, and in the subsequent Corollaries 2.1.12 and 2.1.13 we present two simple applications to binary quadratic Diophantine inequalities.

Recall from Theorem 2.1.3, that every rational number has a continued fraction whose length has a preassigned parity.

Theorem 2.1.10 (Legendre's approximation theorem)**.** *Suppose that $z \in \mathbb{R} \setminus \mathbb{Q}$, $(p, q) \in \mathbb{Z} \times \mathbb{N}$ such that $(p, q) = 1$, and*

$$\frac{p}{q} = [v_0, v_1, \ldots, v_n], \quad \textit{where} \quad n \in \mathbb{N}_0 \ \ \textit{satisfies} \ \ (-1)^n = \operatorname{sgn}\Bigl(z - \frac{p}{q}\Bigr),$$

$v_0 \in \mathbb{Z}$ and $v_1, \ldots, v_n \in \mathbb{N}$. Let $(p_i')_{i \in [-2,n]}$ be the sequence of partial numerators and $(q_i')_{i \in [-2,n]}$ the sequence of partial denominators of the continued fraction $[v_0, \ldots, v_n]$ (hence $p_n' = p$ and $q_n' = q$), and set $q' = q_{n-1}'$. Then

$$\frac{p}{q} \ \ \textit{is a convergent of } z \textit{ if and only if } \ \Bigl| z - \frac{p}{q} \Bigr| < \frac{1}{q(q + q')}.$$

In this case, $p = p_n$ is the n-th partial numerator and $q = q_n$ is the n-th partial denominator of z.

Proof. We set

$$\vartheta = q^2 \Bigl| z - \frac{p}{q} \Bigr|, \quad \text{hence} \quad z = \frac{p}{q} + \frac{(-1)^n \vartheta}{q^2}, \quad \text{and} \quad \vartheta \notin \mathbb{Q}.$$

Since $q \ge q' \ge 0$ and $q \ge 1$, it follows that

$$\frac{1}{2} \le \frac{q}{q + q'} \le 1.$$

CASE 1: $\vartheta > 1$. By Theorem 2.1.3.2,

$$\Bigl| z - \frac{p}{q} \Bigr| = \frac{\vartheta}{q^2} > \frac{1}{q^2} \ge \frac{1}{q(q + q')} \ \text{ implies that } \frac{p}{q} \text{ is not a convergent of } z.$$

CASE 2: $\vartheta < 1$. We set

$$p' = p_{n-1}' \quad \text{and} \quad \omega = \frac{-zq' + p'}{zq - p} \in \mathbb{R} \setminus \mathbb{Q}.$$

Then $p'q-pq'=p'_{n-1}q'_n-p'_nq'_{n-1}=(-1)^n$,

$$z=\frac{p\,\omega+p'}{q\,\omega+q'}\;=\;\frac{p'_n\omega+p'_{n-1}}{q'_n\omega+q'_{n-1}}=[\,v_0,\ldots,v_n,\omega]=\Big[v_0,\ldots,v_{n-1},v_n+\frac{1}{\omega}\Big],$$

and

$$\omega\;=\;\frac{-q'\Big(\dfrac{p}{q}+\dfrac{(-1)^n\vartheta}{q^2}\Big)+p'}{\Big(\dfrac{p}{q}+\dfrac{(-1)^n\vartheta}{q^2}\Big)q-p}\;=\;\frac{-q'pq-(-1)^n\vartheta q'+p'q^2}{pq^2+(-1)^n\vartheta q-pq^2}$$

$$=\;\frac{q(p'q-pq')-(-1)\vartheta q'}{(-1)^n\vartheta q}\;=\;\frac{q-\vartheta q'}{\vartheta q}\,.$$

If $n=0$, then $q'=0$ and $\omega=\vartheta^{-1}>1$. If $n\geq 1$, then $q-\vartheta q'>q-q'\geq 0$. In any case, it follows that

$$\omega>0\,,\quad \vartheta=\frac{q}{q'+q\omega}\,,$$

and therefore

$$\vartheta<\frac{q}{q+q'}\quad\text{if and only if}\quad \omega>1\,.$$

CASE 2a: $\omega>1$. Let $\omega=[v_{n+1},v_{n+2},\ldots]$ be the continued fraction of ω. Then $v_{n+1}=\lfloor\omega\rfloor\geq 1$ and $z=[\,v_0,\ldots,v_n,\omega]=[v_0,\ldots,v_n,v_{n+1},\ldots]$, which implies $p=p_n$ and $q=q_n$.

CASE 2b: $\omega<1$. Then $n\geq 1$, hence $q'\geq 1$, and since $v_n+\omega^{-1}>v_n+1$, we obtain $v_n+\omega^{-1}=[v_n+c,v_{n+1},\ldots]$ for some $c\in\mathbb{N}$. Therefore it follows that $z=[v_0,\ldots,v_{n-1},v_n+c,v_{n+1},\ldots]$, $p_i=p'_i$ and $q_i=q'_i$ for all $i\in[-2,n-1]$, and

$$q_n=(v_n+c)q_{n-1}+q_{n-2}=v_nq'_{n-1}+q'_{n-2}+cq'_{n-1}=q+cq'>q\geq q'=q_{n-1}\,.$$

If $q_{n-1}<q<q_n$, then q cannot be a partial denominator of z. If $q_{n-1}=q$, (that is, $q'_{n-1}=q'_n$), then $n=1$ and $q=q'=1$, which implies $v_1=1$ and $u_0=v_0=p-1$. Hence $z=[p-1,1+c,\ldots]$, and therefore $p-1=(p-1)/1$ is the unique integral convergent of z. Consequently,

$$\frac{p}{q}=\frac{p}{1}\quad\text{is not a convergent of } z. \qquad\square$$

Corollary 2.1.11. *Assume that* $z\in\mathbb{R}\setminus\mathbb{Q}$, $p\in\mathbb{Z}$, $q\in\mathbb{N}$ *and* $(p,q)=1$.

$$\textit{If}\quad\Big|z-\frac{p}{q}\Big|<\frac{1}{2q^2}\,,\quad\textit{then}\quad\frac{p}{q}\quad\textit{is a convergent of}\ z\,.$$

Proof. We apply Theorem 2.1.10. If q' is as there, then

$$\Big|z-\frac{p}{q}\Big|<\frac{1}{2q^2}\leq\frac{1}{q(q+q')}\,,\quad\text{and thus}\quad\frac{p}{q}\quad\text{is a convergent of}\ z\,. \qquad\square$$

Corollary 2.1.12. *Assume that* $z\in\mathbb{R}\setminus\mathbb{Q}$, $p,\,q\in\mathbb{N}$ *and* $(p,q)=1$.

$$\textit{If}\quad|p^2-z^2q^2|<z\,,\quad\textit{then}\quad\frac{p}{q}\quad\textit{is a convergent of}\ z\,.$$

Proof. Let $\vartheta \in \mathbb{R}_{>0}$, $n \in \mathbb{N}_0$, $v_0 \in \mathbb{Z}$ and $v_1, \ldots, v_n \in \mathbb{N}$ be such that

$$z - \frac{p}{q} = \frac{(-1)^n \vartheta}{q^2} \qquad \text{and} \qquad \frac{p}{q} = [v_0, v_1, \ldots, v_n].$$

Let $(p_i')_{i \in [-2,n]}$ be the sequence of partial numerators and $(q_i')_{i \in [-2,n]}$ the sequence of partial denominators of the continued fraction $[v_0, \ldots, v_n]$ (hence $p_n' = p$ and $q_n' = q$), and set $q' = q_{n-1}'$. By Theorem 2.1.10 we must prove that

$$\vartheta < \frac{q}{q+q'}\,.$$

By assumption, we have

$$\vartheta \;=\; q^2 \Big| z - \frac{p}{q} \Big| \;=\; q\,\frac{|q^2z^2 - p^2|}{qz+p} \;<\; \frac{qz}{qz+p} \;<\; 1\,.$$

If $n = 0$, then $q' = 0$, and since $\vartheta < 1$, the assertion follows. Thus assume that $n \geq 1$. It suffices to prove that

$$\frac{qz}{qz+p} \leq \frac{q}{q+q'}\,, \quad \text{which is equivalent to} \quad q' \leq \frac{p}{z} = q - \Big(q - \frac{p}{z}\Big)\,.$$

If $n = 1$, then

$$q - \frac{p}{z} = \frac{q}{z}\Big(z - \frac{p}{q}\Big) < 0 \quad \text{and therefore} \quad q' = q_0' = 1 \leq q < q - \Big(q - \frac{p}{z}\Big)\,.$$

If $n \geq 2$, then

$$\Big| q - \frac{p}{z} \Big| = \frac{q}{z} \Big| z - \frac{p}{q} \Big| = \frac{\vartheta}{qz} < \frac{1}{p+qz} < 1\,, \quad \text{and} \quad q' = q_{n-1}' \leq q - 1 < q - \Big(q - \frac{p}{z}\Big)\,. \;\square$$

Corollary 2.1.13. *Let $D \in \mathbb{N}$ be not a square, and p, $q \in \mathbb{N}$.*

$$\text{If} \quad |p^2 - Dq^2| < \sqrt{D}\,, \quad \text{then} \quad \frac{p}{q} \quad \text{is a convergent of} \quad \sqrt{D}\,.$$

Proof. By Corollary 2.1.12, applied with $z = \sqrt{D}$. □

We close this section concerning general continued fractions with the promised criterion for the equivalence of two irrational real numbers (see the remarks between the Exercises 1.3.6 and 1.3.7).

Theorem 2.1.14 (Equivalence theorem)**.** *Let z, $y \in \mathbb{R} \setminus \mathbb{Q}$ be two irrational real numbers, $(z_i)_{i \geq 0}$ the sequence of complete quotients of z and $(y_i)_{i \geq 0}$ the sequence of complete quotients of y.*

1. *For every $n \geq 0$, z is properly equivalent to $(-1)^n z_n$.*
2. *Let $A \in \mathsf{GL}_2(\mathbb{Z})$ be such that $y = Az$. Then there exist m, $n \in \mathbb{N}_0$ such that $(-1)^{m+n} = \det(A)$ and $z_n = y_m$.*
3. *z is equivalent to y if and only if there exist m, $n \in \mathbb{N}_0$ such that $z_n = y_m$ (and then it follows that $z_{n+i} = y_{m+i}$ for all $i \geq 0$).*

Proof. Let $z = [u_0, u_1, \ldots]$ be the continued fraction, $(p_n)_{n\ge -2}$ the sequence of partial numerators and $(q_n)_{n\ge -2}$ the sequence of partial denominators of z.

1. If $n \ge 0$, then

$$z = [u_0, \ldots, u_{n-1}, z_n] = \frac{p_{n-1}z_n + p_{n-2}}{q_{n-1}z_n + q_{n-2}} = \begin{pmatrix} (-1)^n p_{n-1} & (-1)^n p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} (-1)^n z_n$$

and

$$\det \begin{pmatrix} (-1)^n p_{n-1} & (-1)^n p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} = 1\,.$$

Hence it follows that z is properly equivalent to $(-1)^n z_n$.

2. We may replace A by $-A$, and thus we may assume that

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \qquad \text{and} \qquad \gamma\, z + \delta > 0\,.$$

For $n \ge -2$, we define $p_n^* = \alpha p_n + \beta q_n$ and $q_n^* = \gamma p_n + \delta q_n$. Then p_n^*, $q_n^* \in \mathbb{Z}$,

$$\begin{pmatrix} p_{n+1}^* & p_n^* \\ q_{n+1}^* & q_n^* \end{pmatrix} = A \begin{pmatrix} p_{n+1} & p_n \\ q_{n+1} & q_n \end{pmatrix},$$

and since $p_{n+1}^* q_n^* - p_n^* q_{n+1}^* = (-1)^n \det(A) \in \{\pm 1\}$, it follows that $(p_n^*, q_n^*) = 1$. If $n \ge 1$, then

$$\begin{aligned} q_{n-1}^* &= \gamma p_{n-1} + \delta q_{n-1} = \gamma(u_{n-1}p_{n-2} + p_{n-3}) + \delta(u_{n-1}q_{n-2} + q_{n-3}) \\ &= u_{n-1}q_{n-2}^* + q_{n-3}^*\,. \end{aligned}$$

Since

$$q_n \ge 1\,, \quad q_n^* = q_n\Bigl(\gamma \frac{p_n}{q_n} + \delta\Bigr) \quad \text{for all } n \ge 0 \quad \text{and} \quad \lim_{n\to\infty} \gamma \frac{p_n}{q_n} + \delta = \gamma\, z + \delta > 0\,,$$

there is some $N \ge 3$ such that $q_{n-1}^* = u_{n-1}q_{n-2}^* + q_{n-3}^* > q_{n-2}^* > 0$ (and thus $q_{n-1}^* \ge 2$) for all $n \ge N$.

Assume from now on that $n \ge N$, and consider the continued fraction

$$\frac{p_{n-1}^*}{q_{n-1}^*} = [v_0, v_1, \ldots, v_{m-1}]\,,$$

where $m \in \mathbb{N}$ is such that $(-1)^m = (-1)^n \det(A)$, $v_0 \in \mathbb{Z}$, $v_1, \ldots, v_{m-1} \in \mathbb{N}$ and $m \ge 2$ (since $q_{n-1}^* \ge 2$). Let $(p_j')_{j\in[-2,m-1]}$ be the sequence of partial numerators and $(q_j')_{j\in[-2,m-1]}$ the sequence of partial denominators of the continued fraction $[v_0, v_1, \ldots, v_{m-1}]$. Since $(p_{n-1}^*, q_{n-1}^*) = 1$, we obtain $p_{n-1}^* = p_{m-1}'$, $q_{n-1}^* = q_{m-1}'$, and

$$\begin{aligned} p_{n-1}^* q_{m-2}' - q_{n-1}^* p_{m-2}' &= p_{m-1}' q_{m-2}' - q_{m-1}' p_{m-2}' = (-1)^m = (-1)^n \det(A) \\ &= p_{n-1}^* q_{n-2}^* - q_{n-1}^* p_{n-2}^*\,. \end{aligned}$$

It follows that $p_{n-1}^* q_{m-2}' \equiv p_{n-1}^* q_{n-2}^* \bmod q_{n-1}^*$, hence $q_{m-2}' \equiv q_{n-2}^* \bmod q_{n-1}^*$, and $1 \le q_{m-2}' \le q_{m-1}' = q_{n-1}^*$, since $m \ge 2$. On the other hand, we have $1 \le q_{n-2}^* < q_{n-1}^*$, and therefore we obtain $q'_{m-2} = q^*_{n-2}$, hence $p'_{m-2} = p^*_{n-2}$, and

$$\begin{aligned} y &= Az = A\begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} z_n = \begin{pmatrix} p^*_{n-1} & p^*_{n-2} \\ q^*_{n-1} & q^*_{n-2} \end{pmatrix} z_n \\ &= \begin{pmatrix} p'_{m-1} & p'_{m-2} \\ q'_{m-1} & q'_{m-2} \end{pmatrix} z_n = \frac{p'_{m-1}z_n + p'_{m-2}}{q'_{m-1}z_n + q'_{m-2}} = [v_0, \ldots, v_{m-1}, z_n]\,. \end{aligned}$$

By the uniqueness of the continued fraction of y we conclude that $z_n = y_m$.

3. Obvious by 1., 2., and the uniqueness of the continued fraction. □

Exercise 2.1.15 (Continuation of Exercise 1.3.7)**.** In Exercise 1.3.7 we determined all reduced quadratic irrationals of discriminant $\Delta \in [5, 32]$. Now calculate their continued fractions, group them into classes of (proper) equivalence and determine h_Δ and h^+_Δ for these discriminants.

2.2. Continued fractions of quadratic irrationals I: General theory

By a theorem due to Euler and Lagrange (18th century!) an irrational real number has an (ultimately) periodic continued fraction if and only if it is a quadratic irrational, and by a theorem of Galois, the continued fraction of a quadratic irrational ξ is (purely) periodic if and only if ξ is reduced. These classical results will be summarized in the subsequent periodicity theorem 2.2.2. In the course of its proof, we will also obtain a proof of the hitherto unproved Theorem 1.3.5.1. First, however, let us fix some terminology connected with periodicity.

A sequence $(x_n)_{n\ge0}$ is called *ultimately periodic* if there exist integers $k \in \mathbb{N}_0$ and $l \in \mathbb{N}$ such that $x_{n+l} = x_n$ for all $n \ge k$, and in this case we write

$$(x_n)_{n\ge0} = (x_0, \ldots, x_{k-1}, \overline{x_k, \ldots, x_{k+l-1}})\,.$$

If $l \in \mathbb{N}$ is minimal such that $x_{n+l} = x_n$ for all sufficiently large $n \in \mathbb{N}$, then we call l the *period length* and $(x_k, \ldots, x_{k+l-1})$ the *period* of $(x_n)_{n\ge0}$. If l is the period length of $(x_n)_{n\ge0}$ and $k \in \mathbb{N}_0$ is minimal such that $x_{n+l} = x_n$ for all $n \ge k$, then we call k the *pre-period length* and (in case $k \ge 1$) $(x_0, \ldots, x_{k-1})$ the *pre-period* of $(x_n)_{n\ge0}$. If $k = 0$, then $(x_n)_{n\ge0}$ is called *periodic.* The following simple Lemma 2.2.1 is useful in dealing with period and pre-period lengths.

Lemma 2.2.1. *Let $(x_n)_{n\ge0}$ be an an ultimately periodic sequence with pre-period length k and period length l. For any $k_1 \in \mathbb{N}_0$ and $l_1 \in \mathbb{N}$, the following assertions are equivalent*:

(a) $x_{n+l_1} = x_n$ *for all* $n \ge k_1$.

(b) $k_1 \ge k$ *and* $l \mid l_1$.

Proof. (a) ⇒ (b) Let $\mu, \rho \in \mathbb{N}_0$ be such that $l_1 = l\mu + \rho$ and $\rho < l$. For all sufficiently large $n \in \mathbb{N}$ we then obtain $x_n = x_{n+\mu l+\rho} = x_{n+\rho}$ and thus $\rho = 0$ by the minimality of l. It follows that $x_n = x_{n+\mu l}$ for all $n \ge k_1$, hence also $x_n = x_{n+j\mu l}$ for all $n \ge k_1$ and $j \ge 0$. If $j \in \mathbb{N}$ and $j\mu l \ge k$, then $x_n = x_{n+j\mu l} = x_{n+j\mu l+l} = x_{n+l}$ for all $n \ge k_1$ and therefore $k_1 \ge k$ by the minimality of k. □

Theorem 2.2.2 (Periodicity theorem)**.** *Let* $\xi = [u_0, u_1, \ldots] \in \mathbb{R} \setminus \mathbb{Q}$ *be an irrational number and* $(\xi_n)_{n\geq 0}$ *its sequence of complete quotients.*

1. *For* $k \in \mathbb{N}_0$ *and* $l \in \mathbb{N}$ *the following assertions are equivalent:*
   (a) *The sequence* $(u_n)_{n\geq 0}$ *is ultimately periodic with pre-period length* k *and period length* l*.*
   (b) *The sequence* $(\xi_n)_{n\geq 0}$ *is ultimately periodic with pre-period length* k *and period length* l*.*
   (c) *The numbers* $\xi = \xi_0,\ \xi_1, \ldots, \xi_{k+l-1}$ *are distinct, and* $\xi_{k+l} = \xi_k$*.*
2. (Euler - Lagrange - Galois) *The sequence* $(u_n)_{n\geq 0}$ *is ultimately periodic if and only if* ξ *is a quadratic irrational, and it is periodic if and only if* ξ *is a reduced quadratic irrational.*
3. *Let* ξ *be a quadratic irrational of discriminant* Δ*,* k *the pre-period length and* l *the period length of* $(\xi_n)_{n\geq 0}$*.*
   (a) *For all* $n \geq 0$*,* ξ_n *is a quadratic irrational of discriminant* Δ *which is properly equivalent to* $(-1)^n\xi$*, and if* $n \geq k$*, then* ξ_n *is reduced.*
   (b) *The* l *numbers* $\xi_k,\ \xi_{k+1}, \ldots, \xi_{k+l-1}$ *are all reduced quadratic irrationals which are equivalent to* ξ*.*

   In particular, every real quadratic irrational is properly equivalent to a reduced quadratic irrational (as asserted in the Theorems 1.3.5.1 and 1.3.10).

Proof. Throughout, we make use of the uniqueness of infinite continued fractions (see Theorem 2.1.3).

1. (a) $\Leftrightarrow$ (b) Since $\xi_{n+l} = [u_{n+l}, u_{n+l+1}, \ldots]$ and $\xi_n = [u_n, u_{n+1}, \ldots]$ for all $n,\ l \in \mathbb{N}_0$, it follows that $\xi_{n+l} = \xi_n$ for all $n \geq k$ if and only if $u_{n+l} = u_n$ for all $n \geq k$. Hence (a) and (b) are equivalent.

(a), (b) $\Rightarrow$ (c) By definition, $\xi_{k+l} = \xi_k$, and we must prove that $\xi_i \neq \xi_s$ for all $i,\ s \in [k, k+l-1]$ such that $i \neq s$. Thus suppose that $k \leq i \leq s < k+l$ and $\xi_i = \xi_s$. Then $[u_i, u_{i+1}, \ldots] = [u_s, u_{s+1}, \ldots]$, and therefore $u_n = u_{n+s-i}$ for all $n \geq i$. By Lemma 2.2.1, we obtain $i \geq k$ and $l \mid s-i$, but as $s-i < l$, this implies $s = i$.

(c) $\Rightarrow$ (a) Since $\xi_{k+l} = \xi_k$, it follows that $[u_{k+l}, u_{k+l+1}, \ldots] = [u_k, u_{k+1}, \ldots]$ and therefore $u_n = u_{n+l}$ for all $n \geq k$. Let $k_0 \in \mathbb{N}_0$ be the pre-period length and $l_0 \in \mathbb{N}$ the period length of $(u_n)_{n\geq 0}$. By Lemma 2.2.1 we get $k_0 \leq k$ and $l_0 \mid l$, hence $k + l \geq k_0 + l_0$, and by the already proved implication (a) $\Rightarrow$ (c) it follows that $\xi_{k_0+l_0} = \xi_{k_0}$. Hence $k + l = k_0 + l_0$, which implies $k = k_0$ and $l = l_0$.

2. We proceed in four steps:

a. If $(u_n)_{n\geq 0}$ is periodic, then ξ is a reduced quadratic irrational;

b. If ξ is a reduced quadratic irrational, then $(u_n)_{n\geq 0}$ is periodic;

c. If $(u_n)_{n\geq 0}$ is ultimately periodic, then ξ is a quadratic irrational;

d. If ξ is a quadratic irrational, then $(u_n)_{n\geq 0}$ is ultimately periodic.

a. Let $(u_n)_{n\ge 0}$ be periodic with period length l, $(p_n)_{n\ge -2}$ the sequence of partial numerators and $(q_n)_{n\ge -2}$ the sequence of partial denominators of ξ. Then $u_0 = u_l \ge 1$, $p_{-1} = 1 \le u_0 = p_0$, $q_{-1} = 0 < q_0 = 1 \le q_1 = u_1$, and the sequences $(p_i)_{i\ge 0}$ and $(q_i)_{i\ge 1}$ are strictly monotonically increasing. Since

$$\xi = [u_0, \ldots, u_{l-1}, \xi_l] = [u_0, \ldots, u_{l-1}, \xi] = \frac{p_{l-1}\xi + p_{l-2}}{q_{l-1}\xi + q_{l-2}}\,,$$

it follows that

$$q_{l-1}\xi^2 + (q_{l-2} - p_{l-1})\xi - p_{l-2} = 0\,.$$

Hence ξ is a quadratic irrational, $\xi > u_0 \ge 1$, and the numbers ξ and its conjugate ξ' are the only roots of the polynomial $f = q_{l-1}X^2 + (q_{l-2} - p_{l-1})X - p_{l-2}$. Since $f(-1) = q_{l-1} - q_{l-2} + p_{l-1} - p_{l-2} > 0$ and $f(0) = -p_{l-2} < 0$, it follows that $\xi' \in (-1, 0)$, and therefore ξ is a reduced quadratic irrational.

b. Let ξ be a reduced quadratic irrational of discriminant Δ and $(\xi_n)_{n\ge 0}$ the sequence of complete quotients of ξ. Since $\xi_0 = \xi$ and $\xi_{n+1} = \xi_n^{\#}$ for all $n \ge 0$, Theorem 1.3.5 implies that $(\xi_n)_{n\ge 0}$ is a sequence of reduced quadratic irrationals of discriminant Δ, but by Theorem 1.3.10 there are only finitely many of them. Hence there exist indices $k \in \mathbb{N}_0$ and $l \in \mathbb{N}$ such that $\xi_{k+l} = \xi_k$, and $\xi_0, \xi_1, \ldots, \xi_{k+l-1}$ are distinct. Therefore 1. implies that the sequences $(u_n)_{n\ge 0}$ and $(\xi_n)_{n\ge 0}$ are both ultimately periodic with pre-period length k and period length l. We must prove that $k = 0$, and we assume to the contrary that $k \ge 1$. Then $\xi_{k-1} \ne \xi_{k+l-1}$,

$$\xi_{k+l-1} = u_{k+l-1} + \frac{1}{\xi_{k+l}} = u_{k+l-1} + \frac{1}{\xi_k}\,, \quad \xi_{k-1} = u_{k-1} + \frac{1}{\xi_k}\,,$$

and therefore $\xi_{k+l-1} - \xi_{k-1} = u_{k+l-1} - u_{k-1} \in \mathbb{Z}$. Since $\{\xi_{k+l-1}, \xi_{k-1}\} \subset \mathbb{Q}(\sqrt{\Delta}\,)$, it follows that $\xi'_{k+l-1} - \xi'_{k-1} = (\xi_{k+l-1} - \xi_{k-1})' = \xi_{k+l-1} - \xi_{k-1} \in \mathbb{Z}$, and as $\{\xi'_{k+l-1}, \xi'_{k-1}\} \subset (-1, 0)$, we obtain $\xi'_{k+l-1} = \xi'_{k-1}$, a contradiction.

c. If $(u_n)_{n\ge 0}$ is ultimately periodic with pre-period length $k \in \mathbb{N}_0$, then the sequence $(u_{k+n})_{n\ge 0}$ is periodic, and therefore $\xi_k = [u_k, u_{k+1}, \ldots]$ is a quadratic irrational. Since $\xi \sim_+ (-1)^k\xi_k$, it follows that $\xi \sim \xi_k$, and therefore ξ is a quadratic irrational, too.

d. Let ξ be a quadratic irrational. If $n \ge 1$, then $\xi_n = [u_n, u_{n+1}, \ldots] \sim \xi$, hence ξ_n is also a quadratic irrational, and $\xi_n > u_n \ge 1$. We shall prove that $-1 < \xi'_k < 0$ for some $k \ge 1$. Then the sequence $(u_n)_{n\ge k}$ is periodic, and consequently the sequence $(u_n)_{n\ge 0}$ is ultimately periodic.

Let $(p_n)_{n\ge -2}$ be the sequence of partial numerators and $(q_n)_{n\ge -2}$ the sequence of partial denominators of ξ. For $k \ge 2$ this implies

$$\xi = \frac{p_{k-1}\xi_k + p_{k-2}}{q_{k-1}\xi_k + q_{n-k}}\,, \quad \text{hence } \ \xi_k = \frac{-q_{k-2}\xi + p_{k-2}}{q_{k-1}\xi - p_{k-1}} \quad \text{and} \quad \xi'_k = -\frac{q_{k-2}}{q_{k-1}}\gamma_k\,,$$

where

$$\gamma_k \;=\; \frac{\xi' - \dfrac{q_{k-2}}{q_{k-2}}}{\xi' - \dfrac{p_{k-1}}{q_{k-1}}} \;=\; \frac{\xi' - \dfrac{p_{k-1}}{q_{k-1}} + \dfrac{p_{k-1}}{q_{k-1}} - \dfrac{q_{k-2}}{q_{k-2}}}{\xi' - \dfrac{p_{k-1}}{q_{k-1}}} \;=\; 1 + \frac{(-1)^k}{q_{k-1}q_{k-2}\Big(\xi' - \dfrac{p_{k-1}}{q_{k-1}}\Big)}\,.$$

Since

$$\lim_{k\to\infty}\gamma_k = \frac{\xi'-\xi}{\xi'-\xi} = 1 \quad\text{and}\quad \lim_{k\to\infty}\frac{p_k}{q_k} = \xi\,,$$

there exists some $k_0 \geq 2$ such that

$$\gamma_k > 0 \quad\text{and}\quad \operatorname{sgn}\Bigl(\xi' - \frac{p_{k-1}}{q_{k-1}}\Bigr) = \operatorname{sgn}(\xi'-\xi) \quad\text{for all}\quad k \geq k_0\,.$$

If $k \geq k_0$ is such that $(-1)^k\operatorname{sgn}(\xi'-\xi) = -1$, then it follows that $\gamma_k \in (0,1)$, and

$$-\frac{q_{k-2}}{q_{k-1}} \in (-1,0) \quad\text{implies}\quad \xi_k' = -\frac{q_{k-2}}{q_{k-1}}\gamma_k \in (-1,0)\,.$$

3. (a) We apply 2. and Theorem 2.1.14.1. If $n \geq 0$, then ξ_n is properly equivalent to $(-1)^n\xi$, hence equivalent to ξ, and therefore ξ_n is a quadratic irrational of discriminant Δ. If $n \geq k$ then $\xi_n = [\,\overline{u_n, u_{n+1}, \ldots, u_{n+l-1}}\,]$, and thus ξ_n is reduced.

(b) By 2. and 3.(a), the numbers ξ_k, $\xi_{k+1}, \ldots, \xi_{k+l-1}$ are distinct reduced quadratic irrationals which are equivalent to ξ. Let η be any reduced quadratic irrational which is equivalent to ξ, and let $(\eta_n)_{n\geq 0}$ be the periodic sequence of its complete quotients. By Theorem 2.1.14, there exist indices m, $n \in \mathbb{N}_0$ such that $\xi_n = \eta_m$. Then it follows that $\xi_{n+j} = \eta_{m+j}$ for all $j \geq 0$. Let l be the period length of $(\eta_n)_{n\geq 0}$ and s, r, $j \in \mathbb{N}_0$ such that $sl \geq m$, $n + sl - m = k + rl + j$ and $j < l$. Then we obtain $\eta = \eta_0 = \eta_{sl} = \xi_{n+sl-m} = \xi_{k+j+rl} = \xi_{k+j}$. □

Remarks and Definition 2.2.3. Theorem 2.2.2 causes the following definition. Let $\Delta > 0$ be a quadratic discriminant and ξ a quadratic irrational of discriminant Δ. Let $(\xi_n)_{n\geq 0}$ be the sequence of complete quotients of ξ, k its pre-period length and l its period length. Then we call $\mathsf{z}(\xi) = (\xi_k, \xi_{k+1}, \ldots, \xi_{k+l-1})$ the *period* and $l = l(\xi)$ the *period length* of ξ. By definition, it follows that

$$\mathsf{z}(\xi_{k+j}) = (\xi_{k+j}, \xi_{k+j-1}, \ldots, \xi_{k+l-1}, \xi_k, \ldots, \xi_{k+j-1}) \quad\text{for all } j \in [0, l-1]\,,$$

and the l numbers $\xi_k, \ldots, \xi_{k+l-1}$ are precisely the reduced quadratic irrationals equivalent to ξ.

More generally, a finite sequence $\mathsf{z} = (\xi_0, \ldots, \xi_{l-1})$ of quadratic irrationals of discriminant Δ is called a *period* (of discriminant Δ) if $\mathsf{z} = \mathsf{z}(\xi_0)$ (then ξ_0 is reduced). Two such periods $\mathsf{z}(\xi_0)$ and $\mathsf{z}(\eta_0)$ are called *equivalent* if they are shifts of each other. Explicitly, if $\mathsf{z}(\xi_0) = (\xi_0, \ldots, \xi_{l-1})$ and $\mathsf{z}(\eta_0) = (\eta_0, \ldots, \eta_{m-1})$, then $\mathsf{z}(\xi_0)$ and $\mathsf{z}(\eta_0)$ are equivalent if and only if $l = m$ and there is some $k \in [0, l-1]$ such that $(\eta_0, \ldots, \eta_{l-1}) = (\xi_k, \xi_{k+1}, \ldots, \xi_{l-1}, \xi_0, \ldots, \xi_{k-1})$. By Theorem 2.1.14, the periods $\mathsf{z}(\xi_0)$ and $\mathsf{z}(\eta_0)$ are equivalent if and only if ξ_0 and η_0 are equivalent. Therefore

$$h_\Delta = |\mathfrak{X}_\Delta| \quad \text{is the number of equivalence classes of periods of discriminant } \Delta.$$

If $(\xi_0, \ldots, \xi_{l-1)}$ is any period of discriminant Δ, then we define its *periodic extension* $(\xi_n)_{n\in\mathbb{Z}}$ by setting $\xi_n = \xi_j$ if $n \in \mathbb{Z}$, $j \in [0, l-1]$ and $n \equiv j \bmod l$. By definition, if $(\xi_n)_{n\in\mathbb{Z}}$ is the periodic extension of a period $\mathsf{z}(\xi_0)$, then $(\xi_n)_{n\geq 0}$ is the sequence of complete quotients of ξ_0.

Example 2.2.4 (Short periods)**.**
$l=1:$ Let $\mathsf{z}=(\xi)$ be a period of length 1. Then $\xi=[\,\overline{b}\,]$ for some $b\in\mathbb{N}$, hence

$$\xi=[b,\xi]=b+\frac{1}{\xi}, \quad\text{and therefore}\quad x^2-b\xi-1=0 \;\text{ and }\; \xi=\frac{b+\sqrt{b^2+4}}{2}$$

(see Exercise 2.1.5). Hence ξ is of type $(1,b,-1)$ and discriminant $\Delta=b^2+4$.

$l=2:$ Let $\mathsf{z}=(\xi,\xi_1)$ be a period (note that $\xi\neq\xi_1$). Then $\xi=[\,\overline{a,b}\,]=[a,b,\xi]$ for some a, $b\in\mathbb{N}$ such that $a\neq b$. Hence it follows that

$$\xi=a+\frac{1}{b+\xi^{-1}}\,, \quad\text{and therefore}\quad \xi=\frac{ab+\sqrt{a^2b^2+4ab}}{2b}\,.$$

Consequently, if $d=(a,b)$, then ξ is

$$\text{of type}\quad\Big(\frac{b}{d},\frac{ab}{d},\frac{-a}{d}\Big)\quad\text{and discriminant}\quad\frac{a^2b^2+4ab}{d^2}\,.$$

Exercise 2.2.5. Determine all reduced quadratic irrationals ξ with $l(\xi)=3$.

The following Theorem 2.2.6 comprises a collection of formulas connected with the continued fractions of quadratic irrationals. These formulas are the basis of an efficient algorithm, which is explicitly given in the subsequent Corollary 2.2.7.

Theorem 2.2.6 (Continued fractions of quadratic irrationals)**.** *Let $\Delta>0$ be a quadratic discriminant, $\xi=[u_0,u_1,\ldots]$ a quadratic irrational of discriminant Δ, $(p_n)_{n\geq-2}$ the sequence of partial numerators, $(q_n)_{n\geq-2}$ the sequence of partial denominators and $(\xi_n)_{n\geq0}$ the sequence of complete quotients of ξ. For $n\in\mathbb{N}_0$, let (a_n,b_n,c_n) be the type of ξ_n, and set $a_{-1}=-c_0$.*

1. *The following relations hold for all $n\geq0:$*
   - (a) $b_nb_{n+1}+\Delta=2a_nb_{n+1}u_n+4a_na_{n+1}$.
   - (b) $b_n+b_{n+1}=2a_nu_n$.
   - (c) $\Delta=b_{n+1}^2+4a_na_{n+1}$.
   - (d) $c_n=-a_{n-1}$.
   - (e) $2a_0p_{n-1}-b_0q_{n-1}=b_nq_{n-1}+2a_nq_{n-2}$.
   - (f) $\Delta q_{n-1}=2a_0(p_{n-1}b_n+2p_{n-2}a_n)-b_0(q_{n-1}b_n+2q_{n-2}a_n)$.
   - (g) $(2a_0p_{n-1}-b_0q_{n-1})^2-\Delta q_{n-1}^2=4(-1)^na_0a_n$.
2. *If $n\geq1$, then*

$$\theta_n=\prod_{i=1}^{n-1}\xi_i^{-1}=(-1)^{n-1}(p_{n-2}-q_{n-2}\xi)\,,\quad\textit{and}\quad \mathcal{N}(\theta_n)=\frac{(-1)^{n-1}a_{n-1}}{a_0}\,.$$

Proof. 1. (a), (b) Since

$$\xi_n=u_n+\frac{1}{\xi_{n+1}}\,,\qquad\text{it follows that}\qquad \frac{b_n+\sqrt{\Delta}}{2a_n}=u_n+\frac{2a_{n+1}}{b_{n+1}+\sqrt{\Delta}}\,,$$

which implies $\Delta+b_nb_{n+1}+(b_n+b_{n+1})\sqrt{\Delta}=2a_nu_n(\sqrt{\Delta}+b_{n+1})+4a_na_{n+1}$. Now (a) and (b) follow by the linear independence of $(1,\sqrt{\Delta})$.

(c) Multiply (b) by $-b_{n+1}$ and add the result to (a).

(d) By definition, $a_{-1} = -c_0$. For $n \geq 0$, (c) implies

$$c_{n+1} = \frac{b_{n+1}^2 - \Delta}{4a_{n+1}} = -a_n\,.$$

(e), (f) We start with the relation

$$\frac{b_0 + \sqrt{\Delta}}{2a_0} = \xi = \frac{p_{n-1}\xi_n + p_{n-2}}{q_{n-1}\xi_n + q_{n-2}} = \frac{p_{n-1}b_n + p_{n-1}\sqrt{\Delta} + 2a_n p_{n-2}}{q_{n-1}b_n + q_{n-1}\sqrt{\Delta} + 2a_n q_{n-2}}\,.$$

Cross-multiplication and comparing coefficients implies (e) and (f).

(g) We multiply (e) by $2a_0p_{n-1} - b_0q_{n-1}$, (f) by $-q_{n-1}$ and add the resulting equations to obtain (g).

2. We use induction on n.

$n = 1$: $1 = \theta_1 = p_{-1} - \xi q_{-1}$.

$n \geq 1$, $n \to n+1$: Since

$$\xi = \frac{p_{n-1}\xi_n + p_{n-2}}{q_{n-1}\xi_n + q_{n-2}}\,, \qquad \text{we obtain} \qquad \xi_n^{-1} = \frac{q_{n-1}\xi - p_{n-1}}{-q_{n-2}\xi + p_{n-2}}\,,$$

and the induction hypothesis implies

$$\prod_{i=1}^{n} \xi_i^{-1} = (-1)^{n-1}(p_{n-2} - q_{n-2}\xi)\,\xi_n^{-1} = (-1)^n(p_{n-1} - q_{n-1}\xi)\,.$$

By Theorem 1.1.2.2 and 2.(d) it follows that

$$\mathcal{N}(\theta_n) = \prod_{i=1}^{n-1} \mathcal{N}(\xi_i)^{-1} = \prod_{i=1}^{n-1}\Big(\frac{c_i}{a_i}\Big)^{-1} = \prod_{i=1}^{n-1}\Big(\frac{-a_i}{a_{i-1}}\Big) = \frac{(-1)^{n-1}a_{n-1}}{a_0}\,. \qquad \square$$

Corollary 2.2.7 (Continued fraction algorithm)**.** *Let $\Delta > 0$ be a quadratic discriminant and ξ a quadratic irrational of type (a,b,c) and discriminant Δ. Let the sequences $(a_n)_{n\geq 0}$, $(b_n)_{n\geq 0}$, $(\xi_n)_{n\geq 0}$ and $(u_n)_{n\geq 0}$ be recursively defined by $a_0 = a$, $b_0 = b$,*

$$\xi_n = \frac{b_n + \sqrt{\Delta}}{2a_n}\,, \quad u_n = \lfloor \xi_n \rfloor\,, \quad b_{n+1} = -b_n + 2a_nu_n \quad \text{and} \quad a_{n+1} = \frac{\Delta - b_{n+1}^2}{4a_n}$$

for all $n \geq 0$. Then $\xi = [u_0, u_1, \ldots]$, and $(\xi_n)_{n\geq 0}$ is the sequence of complete quotients of ξ.

Proof. Obvious by Theorem 2.2.6. ☐

Exercise 2.2.8. Calculate the continued fraction of $\xi = (5 + \sqrt{24})/2$ using the algorithm given by Corollary 2.2.7. Observe that ξ is of type $(4, 20, 1)$.

We conclude this section with a thorough theory of Pell's equation using the continued fraction of reduced quadratic irrationals. This approach will not only furnish a new proof of the existence of infinitely many solutions (see Theorem 1.2.3), but we will also obtain a deep insight into the structure of the set of solutions.

Theorem 2.2.9 (Pell's equation)**.** *Let $\Delta > 0$ be a quadratic discriminant, ξ a reduced quadratic irrational of discriminant Δ, $l = l(\xi)$ its period length and*

$$\xi = [u_0, u_1, \ldots] = [\,\overline{u_0, u_1, \ldots, u_{l-1}}\,]$$

its continued fraction. Let $(\xi_0, \ldots, \xi_{l-1})$ be the period, $(p_n)_{n\ge -2}$ the sequence of partial numerators and $(q_n)_{n\ge -2}$ the sequence of partial denominators of ξ. We consider the quadratic irrational

$$\varepsilon_\Delta = \prod_{i=0}^{l-1} \xi_i \in \mathbb{Q}(\sqrt{\Delta}\,)\,.$$

1. *For all $m \in \mathbb{N}_0$ we have*

$$\varepsilon_\Delta^m = \prod_{i=0}^{ml-1} \xi_i \;=\; q_{ml-1}\xi + q_{ml-2} = \frac{(-1)^{ml}}{p_{ml-1} - q_{ml-1}\xi}\,, \quad \mathcal{N}(\varepsilon_\Delta^m) = (-1)^{ml}\,,$$

and ε_Δ^m is a zero of the polynomial $X^2 - (p_{ml-1} + q_{ml-2})X + (-1)^{ml}$.

2. (Solution set of Pell's equation)

$$\Big\{\frac{u + v\sqrt{\Delta}}{2} \;\Big|\; u,\, v \in \mathbb{N}_0\,,\ |u^2 - \Delta v^2| = 4\Big\} = \{q_{ml-1}\xi + q_{ml-2} \mid m \in \mathbb{N}_0\}$$
$$= \{\varepsilon_\Delta^m \mid m \in \mathbb{N}_0\} \subset \mathbb{Q}(\sqrt{\Delta}\,)^\times\,,$$

and

$$\Big\{\frac{u + v\sqrt{\Delta}}{2} \;\Big|\; u,\, v \in \mathbb{Z}\,,\ |u^2 - \Delta v^2| = 4\Big\} = \langle -1, \varepsilon_\Delta\rangle$$
$$= \{\pm\varepsilon_\Delta^m \mid m \in \mathbb{Z}\} \subset \mathbb{Q}(\sqrt{\Delta}\,)^\times\,.$$

In particular,

$$\varepsilon_\Delta = \frac{u + v\sqrt{\Delta}}{2} \quad \text{with} \quad u,\, v \in \mathbb{N}\,, \quad \varepsilon_\Delta > 1\,, \quad \mathcal{N}(\varepsilon_\Delta) = (-1)^l\,,$$

and Pell's minus equation $x^2 - \Delta y^2 = -4$ has an integral solution if and only if $\mathcal{N}(\varepsilon_\Delta) = -1$.

3. *The quadratic irrational ε_Δ and the parity $l + 2\mathbb{Z} \in \mathbb{Z}/2\mathbb{Z}$ of the period length $l(\xi)$ only depend on Δ (and not on ξ).*
4. *If Y denotes the set of all reduced quadratic irrationals of discriminant Δ, then*

$$\prod_{\eta \in Y} \eta \;=\; \varepsilon_\Delta^{h_\Delta}\,.$$

Proof. Since $\xi_i \in \mathbb{Q}(\sqrt{\Delta}\,)$ and $\xi_i > 1$ for all $i \in [0, l-1]$, it follows that $\varepsilon_\Delta \in \mathbb{Q}(\sqrt{\Delta}\,)$ and $\varepsilon_\Delta > 1$. Let $(\xi_n)_{n\in\mathbb{Z}}$ be the periodic extension of $(\xi_0, \ldots, \xi_{l-1})$. Then $(\xi_n)_{n\ge 0}$ is the sequence of complete quotients of ξ.

1. For $m \in \mathbb{N}_0$, we obtain $u_i = u_{i+ml}$ for all $i \ge 0$, hence

$$\xi = [u_0, u_1, \ldots, u_{ml-1}, \xi] = \frac{p_{ml-1}\xi + p_{ml-2}}{q_{ml-1}\xi + q_{ml-2}}\,, \tag{1}$$

and therefore $q_{ml-1}\xi^2-(p_{ml-1}-q_{ml-2})\xi-p_{ml-2}=0$. Theorem 2.2.6.2 implies

$$\varepsilon_\Delta^m=\Bigl(\prod_{i=0}^{l-1}\xi_i\Bigr)^m=\prod_{i=0}^{lm-1}\xi_i=\prod_{i=1}^{lm}\xi_i=\frac{(-1)^{ml}}{p_{ml-1}-q_{ml-1}\xi}\,,$$

and since

$$\begin{aligned}(p_{ml-1}&-q_{ml-1}\xi)(q_{ml-1}\xi+q_{ml-2})\\&=p_{ml-1}q_{ml-2}-q_{ml-1}[q_{ml-1}\xi^2-(p_{ml-1}-q_{ml-2})\xi]\\&=\ p_{ml-1}q_{ml-2}-q_{ml-1}p_{ml-2}=(-1)^{ml}\,,\end{aligned}$$

it follows that

$$\varepsilon_\Delta^m=\frac{(-1)^{ml}}{p_{ml-1}-q_{ml-1}\xi}=q_{ml-1}\xi+q_{ml-2}\,.$$

By (1), we obtain $\varepsilon_\Delta^m\xi=(q_{ml-1}\xi+q_{ml-2})\xi=p_{ml-1}\xi+p_{ml-2}$ and the eigenvalue equation

$$\varepsilon_\Delta^m\begin{pmatrix}\xi\\1\end{pmatrix}=\begin{pmatrix}p_{ml-1}&p_{ml-2}\\q_{ml-1}&q_{ml-2}\end{pmatrix}\begin{pmatrix}\xi\\1\end{pmatrix}\,.$$

Hence ε_Δ^m is a zero of the polynomial

$$\det\begin{pmatrix}X-p_{ml-1}&-p_{ml-2}\\-q_{ml-1}&X-q_{ml-2}\end{pmatrix}=X^2-(p_{ml-1}+q_{ml-2})X+(-1)^{ml}\,,$$

and therefore $\mathcal{N}(\varepsilon_\Delta^m)=(-1)^{ml}$.

2. Let (a,b,c) be the type of ξ. Then $a>0$, $0<b<\sqrt{\Delta}$, $2a+b>\sqrt{\Delta}$ and $\Delta=b^2-4ac$. If $m\in\mathbb{N}$, then $q_{ml-1}\xi^2-(p_{ml-1}-q_{ml-2})\xi-p_{ml-2}=0$ by (1). By Theorem 1.1.2.2 there is some $v\in\mathbb{Z}$ such that $av=q_{ml-1}$, $bv=p_{ml-1}-q_{ml-2}$ and $cv=-p_{ml-2}$, hence

$$\varepsilon_\Delta^m=q_{ml-1}\xi+q_{ml-2}=av\frac{b+\sqrt{\Delta}}{2a}+q_{ml-2}=\frac{u+v\sqrt{\Delta}}{2}\,,$$

where $u=bv+2q_{ml-2}\in\mathbb{Z}$, and we assert that $u,\,v\in\mathbb{N}_0$.

Indeed, if $m=0$, then $av=q_{-1}=0$, hence $v=0$ and $u=2q_{-2}=2$. If $m>0$, then $av=q_{ml-1}>0$, hence $v>0$, and $b>0$ implies $u=bv+2q_{ml-2}\geq bv>0$.

Since $u^2-\Delta v^2=4\mathcal{N}(\varepsilon_\Delta^m)=4(-1)^{ml}$, it follows that

$$\Bigl\{\frac{u+v\sqrt{\Delta}}{2}\Bigm| u,\,v\in\mathbb{N}_0,\ \ |u^2-\Delta v^2|=4\Bigr\}\supset\{q_{ml-1}\xi+q_{ml-2}\mid m\in\mathbb{N}_0\}\,.$$

For the proof of the reverse inclusion, let $u,\,v\in\mathbb{N}_0$ be such that $|u^2-\Delta v^2|=4$. Then $u\equiv\Delta v\equiv bv \bmod 2$, and $u\neq0$ since Δ is not a square. If $v=0$, then $u=2$, and

$$\frac{u+v\sqrt{\Delta}}{2}=1=\varepsilon_\Delta^0\,.$$

Thus we may assume that $v\geq1$. We set

$$p=\frac{u+bv}{2}\,,\quad p'=-cv\,,\quad q=av\,,\quad q'=\frac{u-bv}{2}\quad\text{and}\quad A=\begin{pmatrix}p&p'\\q&q'\end{pmatrix}\,.$$

Then $p,\,q \in \mathbb{N}$, $p',\,q' \in \mathbb{Z}$, $4\,\det(A) = 4(pq'-qp') = u^2-b^2v^2+4acv^2 = u^2-\Delta v^2$ and $A \in \mathrm{Stab}(\xi)$ by Theorem 1.2.2. We consider the continued fraction

$$\frac{p}{q} = [v_0, v_1, \ldots, v_{k-1}]\,,$$

where $k \in \mathbb{N}$, $v_0 \in \mathbb{N}_0$, $v_1, \ldots, v_k \in \mathbb{N}$ and $(-1)^k = \det(A)$. Let $(p_i')_{i\in[-2,k-1]}$ be the sequence of partial numerators and $(q_i')_{i\in[-2,k-1]}$ the sequence of partial denominators of $[v_0, \ldots, v_{k-1}]$. In particular, $p_{k-1}' = p$, $q_{k-1}' = q$ and

$$pq'-qp' = \det(A) = (-1)^k = p_{k-1}'q_{k-2}' - p_{k-2}'q_{k-1}' = pq_{k-2}' - qp_{k-2}'\,.$$

Hence $pq_{k-2}' \equiv pq' \bmod q$, and since $(p,q) = 1$, we obtain $q_{k-2}' \equiv q' \bmod q$. As $u+v\sqrt{\Delta} \ge 1+\sqrt{\Delta} > 2$, it follows that

$$q' = \frac{u-bv}{2} > \frac{u-v\sqrt{\Delta}}{2} = \frac{2\,\det(A)}{u+v\sqrt{\Delta}} > \begin{cases} 0 & \text{if} \quad \det(A) = 1\,, \\ -1 & \text{if} \quad \det(A) = -1\,, \end{cases}$$

and

$$q-q' = \frac{2av-u+bv}{2} > \frac{-u+v\sqrt{\Delta}}{2} = \frac{-2\,\det(A)}{u+v\sqrt{\Delta}} > \begin{cases} -1 & \text{if} \quad \det(A) = 1\,, \\ 0 & \text{if} \quad \det(A) = -1\,. \end{cases}$$

Thus we obtain $0 < q' \le q$ if $\det(A) = 1$, and $0 \le q' < q$ if $\det(A) = -1$.

If $k = 1$, then $q = 1$, $\det(A) = -1$, $q' = 0$, $a = v = 1$, $u = b$, and

$$\frac{u+v\sqrt{\Delta}}{2} = \frac{b+\sqrt{\Delta}}{2} = \xi = q_0\xi + q_{-1}\,.$$

Thus assume that $k \ge 2$. Then $0 < q_{k-2}' \le q$, hence $q_{k-2}' = q'$, $p_{k-2}' = p'$ and

$$[v_0, \ldots, v_{k-1}, \xi] = \frac{p_{k-1}'\xi + p_{k-2}'}{q_{k-1}'\xi + q_{k-2}'} = \frac{p\xi + p'}{q\xi + q'} = A\xi = \xi\,.$$

Consequently, $\xi = [\,\overline{v_0, \ldots, v_{k-1}}\,]$, and Lemma 2.2.1 implies $l \mid k$. If $k = lm$, where $m \in \mathbb{N}$, then

$$\frac{u+v\sqrt{\Delta}}{2} = \frac{2q'+bv+v\sqrt{\Delta}}{2} = \frac{bav+av\sqrt{\Delta}}{2a} + q' = q\xi + q' = q_{lm-1}\xi + q_{lm-2}\,.$$

Therefore we have proved that

$$\Bigl\{\frac{u+v\sqrt{\Delta}}{2} \Bigm| u,\,v \in \mathbb{N}_0,\ \ |u^2-\Delta v^2| = 4\Bigr\} \ = \ \{q_{ml-1}\xi + q_{ml-2} \mid m \in \mathbb{N}_0\}\,.$$

If $m \in \mathbb{N}_0$ and

$$\varepsilon_\Delta^m = \frac{u+v\sqrt{\Delta}}{2}\,, \quad \text{where} \quad u,\,v \in \mathbb{N}_0\,,$$

then

$$\frac{u-v\sqrt{\Delta}}{2} = (-1)^{lm}\varepsilon_\Delta^{-m}, \quad \frac{-u+v\sqrt{\Delta}}{2} = (-1)^{lm+1}\varepsilon_\Delta^{-m} \ \text{ and } \ \frac{-u-v\sqrt{\Delta}}{2} = -\varepsilon_\Delta^m\,.$$

Gathering these facts, we obtain

$$\Bigl\{\frac{u+v\sqrt{\Delta}}{2} \Bigm| u,\,v \in \mathbb{Z}\,,\ \ |u^2-v^2\Delta| = 4\Bigr\} = \langle -1, \varepsilon_\Delta\rangle \ = \ \{\pm\varepsilon_\Delta^m \mid m \in \mathbb{Z}\}\,.$$

If there exist $x,\, y \in \mathbb{Z}$ such that $x^2 - \Delta y^2 = -4$, then there is some $m \in \mathbb{Z}$ such that

$$\frac{x+y\sqrt{\Delta}}{2} = \varepsilon_\Delta^m\,, \quad \text{and} \quad -1 = \frac{x^2-\Delta y^2}{4} = \mathcal{N}(\varepsilon_\Delta^m) = \mathcal{N}(\varepsilon_\Delta)^m\,,$$

which implies $\mathcal{N}(\varepsilon_\Delta) = -1$. Conversely, if $\mathcal{N}(\varepsilon_\Delta) = -1$, then there exist $u,\, v \in \mathbb{N}$ such that

$$\varepsilon_\Delta = \frac{u+v\sqrt{\Delta}}{2}\,, \quad \text{and then} \quad u^2 - v^2\Delta = 4\mathcal{N}(\varepsilon_\Delta) = -4\,.$$

3. By 2., since Pell's equation only depends on Δ.

4. Let $\eta^{(1)}, \ldots, \eta^{(h)}$ be a complete system of pairwise not equivalent reduced quadratic irrationals of discriminant Δ. For $j \in [1,h]$, let $l_j = l(\eta^{(j)})$ be the period length and $(\eta_n^{(j)})_{n\in[0,l_j-1]}$ the period of $\eta^{(j)}$. By Theorem 2.2.2.3 (b) we obtain $Y = \{\eta_n^{(j)} \mid j \in [1,h]\,,\ n \in [0, l_j-1]\,\}$, and therefore

$$\prod_{\eta\in Y} \eta = \prod_{j=1}^{h} \Bigl(\prod_{i=0}^{l_j-1} \eta_i^{(j)}\Bigr) = \prod_{j=1}^{h} \varepsilon_\Delta = \varepsilon_\Delta^h\,. \qquad \square$$

The number ε_Δ introduced in Theorem 2.2.9 is called the *fundamental unit* of discriminant Δ (this terminology will be justified by the theory of quadratic orders in Theorem 5.2.1). It is of the form

$$\varepsilon_\Delta = \frac{u_0+v_0\sqrt{\Delta}}{2} > 1\,, \quad \text{where} \ \ u_0,\, v_0 \in \mathbb{N}\,, \quad u_0 \equiv v_0\Delta \mod 2\,,$$

and

$$\mathcal{N}(\varepsilon_\Delta) = \frac{u_0^2 - v_0^2\Delta}{4} = (-1)^l\,.$$

For all $n \in \mathbb{Z}$, we have

$$\varepsilon_\Delta^n = \frac{u_n+v_n\sqrt{\Delta}}{2}\,, \quad \text{where} \ \ u_n,\, v_n \in \mathbb{Z}\,,\ u_n \equiv v_n\Delta \mod 2\,, \quad \text{and}$$

$$\mathcal{N}(\varepsilon_\Delta^n) = (-1)^{ln}\,.$$

Using the sequences $(u_n)_{n\in\mathbb{Z}}$ and $(v_n)_{n\in\mathbb{Z}}$, we may describe the solutions of Pell's equation:

$$\{(u_n, v_n) \mid n \in \mathbb{Z}\} = \bigl\{(u,v) \in \mathbb{Z}^2 \bigm| |u^2 - v^2\Delta| = 4\bigr\}\,,$$

$$\{(u_n, v_n) \mid n \in \mathbb{N}\} = \bigl\{(u,v) \in \mathbb{N}^2 \bigm| |u^2 - v^2\Delta| = 4\bigr\}\,,$$

and if $\mathcal{N}(\varepsilon_\Delta) = -1$, then

$$\{(u_{2n+1}, v_{2n+1}) \mid n \in \mathbb{Z}\} = \{(u,v) \in \mathbb{Z}^2 \mid u^2 - v^2\Delta = -4\}\,.$$

Theorem 2.2.9 suggests the following algorithm for the calculation of the fundamental unit ε_Δ.

- `Input some quadratic irrational` ξ_0 `with discriminant` $\Delta > 0$.
- `Calculate the consecutive successors` $\xi_n = \xi_n^{\#}$ `for` $n \ge 1$ `until` $\xi_n = \xi_m$ `for some` $m \in [0, n-1]$.

- Set
$$\varepsilon_\Delta = \prod_{j=m}^{n-1} \xi_j \,.$$

We illustrate the algorithm by considering the discriminant $\Delta = 4(d^2-2)$ for some $d \in \mathbb{N}_{>2}$. We start with $\xi_0 = \sqrt{d^2-2}$ and obtain

$$\xi_0 = \sqrt{d^2-2}\,, \quad \xi_1 = \frac{d-1+\sqrt{d^2-2}}{2d-3}, \quad \xi_2 = \frac{d-2+\sqrt{d^2-2}}{2},$$
$$\xi_3 = \frac{d-2+\sqrt{d^2-2}}{2d-3}, \quad \xi_4 = d-1+\sqrt{d^2-2}, \quad \xi_5 = \xi_1 \,.$$

Hence we get $\varepsilon_\Delta = \xi_1\xi_2\xi_3\xi_4 = d^2-1+d\sqrt{d^2-2}$. For $d=2$, we obtain

$$\xi_0 = \sqrt{2}, \quad \xi_1 = 1+\sqrt{2}, \quad \xi_2 = \frac{\sqrt{2}}{2}, \quad \xi_3 = \xi_0\,,$$

and therefore $\varepsilon_8 = \xi_0\xi_1\xi_2 = 1+\sqrt{2}$.

In the next section we shall investigate the period of the basis number ω_Δ more closely and obtain an algorithm for the calculation of ε_Δ with less effort.

Example 2.2.10. 1. The following table lists all reduced quadratic irrationals of discriminant $\Delta \in [5,32]$ (see Exercise 1.3.7). For each of these discriminants, there is only one cycle (see Exercise 2.1.15), hence $h_\Delta = 1$. Therefore ε_Δ is in each case the product of all reduced irrationals of discriminant Δ, $h_\Delta^+ = 2$ if $\mathcal{N}(\varepsilon_\Delta) = 1$ and $h_\Delta^+ = 1$ if $\mathcal{N}(\varepsilon_\Delta) = -1$ (see Theorem 1.3.10 and observe that Pell's minus equation has integral solutions if and only if $\mathcal{N}(\varepsilon_\Delta) = -1$).

Δ	reduced ξ	ε_Δ	$\mathcal{N}(\varepsilon_\Delta)$	h_Δ	h_Δ^+
5	$\frac{1+\sqrt{5}}{2}$	$\frac{1+\sqrt{5}}{2}$	-1	1	1
8	$1+\sqrt{2}$	$1+\sqrt{2}$	-1	1	1
12	$1+\sqrt{3}\,,\ \frac{1+\sqrt{3}}{2}$	$2+\sqrt{3}$	1	1	2
13	$\frac{3+\sqrt{13}}{2}$	$\frac{3+\sqrt{13}}{2}$	-1	1	1
17	$\frac{1+\sqrt{17}}{4}\,,\ \frac{3+\sqrt{17}}{2}\,,\ \frac{3+\sqrt{17}}{4}$	$4+\sqrt{17}$	-1	1	1
20	$2+\sqrt{5}$	$2+\sqrt{5}$	-1	1	1
21	$\frac{3+\sqrt{21}}{2}\,,\ \frac{3+\sqrt{21}}{6}$	$\frac{5+\sqrt{21}}{2}$	1	1	2
24	$2+\sqrt{6}\,,\ \frac{2+\sqrt{6}}{2}$	$5+\sqrt{24}$	1	1	2
28	$\frac{1+\sqrt{7}}{2}\,,\ 2+\sqrt{7}\,,\ \frac{2+\sqrt{7}}{3}\,,\ \frac{1+\sqrt{7}}{2}$	$5+3\sqrt{7}$	1	1	2
29	$\frac{5+\sqrt{29}}{2}$	$\frac{5+\sqrt{29}}{2}$	-1	1	1
32	$2+2\sqrt{2}\,,\ \frac{1+\sqrt{2}}{2}$	$3+2\sqrt{2}$	1	1	2

The class numbers for positive discriminants $\Delta \le 500$ are listed at the end of Chapter 1. For more extensive tables we refer to the books [**74**] and [**27**].

2. We give a more involved example and consider the discriminant $\Delta = 316$. There are 16 types (a,b,c) satisfying

$$b^2-4ac = 316 \quad \text{and} \quad 0 < \sqrt{316}-b < 2a < \sqrt{316}+b\,.$$

The corresponding reduced quadratic irrationals of discriminant 316 form 3 periods, namely

$$\Bigl(\frac{6+\sqrt{316}}{20},\ \frac{14+\sqrt{316}}{6},\ \frac{16+\sqrt{316}}{10},\ \frac{14+\sqrt{316}}{12},\ \frac{10+\sqrt{316}}{18},\ \frac{8+\sqrt{316}}{14}\Bigr),$$

$$\Bigl(\frac{6+\sqrt{316}}{14},\ \frac{8+\sqrt{316}}{18},\ \frac{10+\sqrt{316}}{12},\ \frac{14+\sqrt{316}}{10},\ \frac{16+\sqrt{316}}{6},\ \frac{14+\sqrt{316}}{20}\Bigr),$$

$$\Bigl(\frac{14+\sqrt{316}}{4},\ \frac{14+\sqrt{316}}{30},\ \frac{16+\sqrt{316}}{2},\ \frac{16+\sqrt{316}}{30}\Bigr).$$

Their continued fractions are given by

$$\frac{6+\sqrt{316}}{20}=[\,\overline{1,5,3,2,1,1}\,],\ \frac{6+\sqrt{316}}{14}=[\,\overline{1,1,2,3,5,1}\,],\frac{14+\sqrt{316}}{4}=[\,\overline{7,1,16,1}\,].$$

Multiplication of the numbers in one of these periods yields

$$\varepsilon_{316}=\frac{160+9\sqrt{316}}{2}=80+9\sqrt{79}\quad\text{and}\quad \mathcal{N}(\varepsilon_{316})=1\,.$$

Therefore $h_{316}=3$ and $h^+_{316}=6$.

Exercise 2.2.11. Calculate all periods, the fundamental units and the class numbers for the discriminants $\Delta=145$ and $\Delta=401$.

In the final theorem of this section we show that in every proper equivalence class of a quadratic irrational there are representatives with specific properties. This result has consequences for the theory of class groups to be discussed in Chapter 5 and the theory of binary quadratic forms in Chapter 6. For negative discriminants, this result could equally have been presented in Chapter 1; for positive discriminants however, we make use of reduction by continued fractions.

Theorem 2.2.12. *Let ξ be a quadratic irrational of type (a,b,c). For every positive integer M, there exists a quadratic irrational ξ_1 of type (a_1,b_1,c_1) such that ξ_1 is properly equivalent to ξ, $(a_1,M)=1$, and $a_1\geq M$ unless $\xi\in\mathfrak{H}^-$.*

Proof. If $\Delta<0$, then ξ is equivalent to a reduced quadratic irrational by Theorem 1.3.2, and since $\xi\notin\mathfrak{H}^-$, it is even properly equivalent to a reduced quadratic irrational. If $\Delta>0$, then ξ is properly equivalent to a reduced quadratic irrational by Theorem 2.2.2. Hence we may assume that ξ is reduced and thus $a>0$. Let M be a positive integer. For $N\in\mathbb{N}$, we define

$$\gamma=\prod_{\substack{p\in\mathbb{P}\\ p\,|\,M,\ p\nmid a}}p\,,\qquad \delta_1=\prod_{\substack{p\in\mathbb{P}\\ p\,|\,(a,M),\ p\nmid c}}p\qquad\text{and}\quad \delta=\delta_1+MN\gamma\,.$$

Then $(\gamma,\delta_1)=1$ by definition, hence $(\gamma,\delta)=1$, and there exist α, $\beta\in\mathbb{Z}$ such that $\alpha\delta-\beta\gamma=1$. We set

$$\xi_1=\begin{pmatrix}\alpha&\beta\\ \gamma&\delta\end{pmatrix}\xi\,.$$

Then ξ_1 is properly equivalent to ξ. We assert that ξ_1 is of some type (a_1, b_1, c_1) such that $(a_1, M) = 1$, and if N is sufficiently large, then $a \geq M$. For this, we calculate

$$\begin{aligned}\xi_1 &= \frac{\alpha\xi+\beta}{\gamma\xi+\delta} = \frac{\alpha\,\frac{b+\sqrt{\Delta}}{2a}+\beta}{\gamma\,\frac{b+\sqrt{\Delta}}{2a}+\delta} = \frac{\alpha b+2a\beta+\alpha\sqrt{\Delta}}{\gamma b+2a\delta+\gamma\sqrt{\Delta}} \\ &= \frac{(\alpha b+2a\beta+\alpha\sqrt{\Delta})(\gamma b+2a\delta-\gamma\sqrt{\Delta})}{(\gamma b+2a\delta)^2-\gamma^2\Delta} \\ &= \frac{2a\beta\delta+b(\alpha\delta+\beta\gamma)+2c\alpha\gamma+\sqrt{\Delta}}{2(a\delta^2+b\gamma\delta+c\gamma^2)}\,.\end{aligned}$$

By Theorem 1.1.2.3, ξ_1 is of type (a_1, b_1, c_1), where $a_1 = a\delta^2 + b\gamma\delta + c\gamma^2$, and we assume, contrary to our assertion, that there is a prime p such that $p \,|\, (a_1, M)$. If $p \,|\, \gamma$, then $p \nmid a$ and thus $p \,|\, \delta$, a contradiction. If $p \,|\, \delta$, then $p \,|\, \delta_1$, hence $p \nmid c$ and therefore $p \,|\, \gamma$, a contradiction. If finally $p \nmid \gamma$ and $p \nmid \delta$, then $p \nmid \delta_1$, hence $p \,|\, a$ and $p \,|\, c$, and since $p \nmid \gamma\delta$, it follows that $p \,|\, b$, again a contradiction. Since $a > 0$, we obtain

$$\lim_{y\to\infty} ay^2 + b\gamma y + ac\gamma^2 = \infty\,.$$

Hence it follows that $a_1 = a\delta^2 + b\gamma\delta + c\gamma^2 \geq M$, provided that δ is sufficiently large, but $\delta = \delta_1 + MN\gamma$ becomes arbitrary large with N. □

2.3. Continued fractions of quadratic irrationals II: Special types

We introduce symmetric and (weakly) ambiguous quadratic irrationals. In the case of positive discriminants, we study their continued fractions and determine the structure of their periods (Theorem 2.3.4). These results are of interest for themselves, but they also have important implications for the theory of class groups (to be discussed in Chapter 5) and for the theory of binary quadratic forms (to be discussed in Chapter 6).

As a special case, we investigate the continued fraction of the basis number of a given quadratic discriminant and apply it to describe once more the solutions of Pell's equation.

Definition 2.3.1. Let Δ be a quadratic discriminant. A quadratic irrational ξ of type (a, b, c) and discriminant Δ is called

- *symmetric* if $c = -a$;
- *ambiguous* if $a \,|\, b$;
- *weakly ambiguous* if $\xi \sim \xi'$.

If $\Delta = 4D + \sigma_\Delta$, where $D \in \mathbb{N}$ and $\sigma_\Delta \in \{0, 1\}$, then the basis number ω_Δ is of type $(1, \sigma_\Delta, D)$, and thus it is ambiguous.

If a quadratic irrational ξ is both ambiguous and symmetric, then it is of type $(a, b, -a)$ with $a \,|\, b$. Hence $a = \pm 1$, and therefore ξ is both ambiguous and symmetric if and only if

$$\xi = \pm\theta_b\,, \quad \text{where} \quad \theta_b = \frac{b+\sqrt{b^2+4}}{2}\,.$$

We have already seen (in Exercise 2.1.5 and Example 2.2.4) that $\theta_b = [\,\overline{b}\,]$, and $-\theta_b = -b + \theta_b^{-1}$ implies $-\theta_b = [-b, \overline{b}\,]$. In particular, $l(\theta_b) = l(-\theta_b) = 1$.

In the next theorem we gather the elementary properties of symmetric, ambiguous and weakly ambiguous real quadratic irrationals.

Theorem 2.3.2. *Let $\Delta > 0$ be a quadratic discriminant, ξ a quadratic irrational of type (a, b, c) and discriminant Δ and $\xi^\#$ its successor.*

1. *The following assertions are equivalent:*
   (a) *ξ is symmetric.*
   (b) *$\xi = -\xi'^{-1}$.*
   (c) *$\mathcal{N}(\xi) = -1$.*
   (d) *$\Delta = 4a^2 + b^2$.*

   If ξ is symmetric, then ξ is reduced if and only if $a, b \in \mathbb{N}$.
2. *Then the following assertions are equivalent:*
   (a) *ξ is ambiguous.*
   (b) *$\xi + \xi' \in \mathbb{Z}$.*
   (c) *$\xi' + (\xi^\#)^{-1} \in \mathbb{Z}$.*

   In particular, if $\xi^\# = -\xi'^{-1}$, then ξ is ambiguous, and if ξ is ambiguous and reduced, then $\xi^\# = -\xi'^{-1}$.
3. *If ξ is either ambiguous or symmetric, then ξ is weakly ambiguous, and if ξ is weakly ambiguous, then $\xi^\#$ is also weakly ambiguous.*

PROOF. 1. (a) $\Leftrightarrow$ (b) As $-\xi'^{-1}$ is of type $(-c, b, -a)$, it follows that $\xi = -\xi'^{-1}$ if and only if $c = -a$.

(b) $\Leftrightarrow$ (c) $\mathcal{N}(\xi) = \xi\xi' = -1$ if and only if $\xi = -\xi'^{-1}$.

(a) $\Leftrightarrow$ (d) From $\Delta = b^2 - 4ac$ we obtain $\Delta = 4a^2 + b^2$ if and only if $c = -a$.

Assume now that ξ is symmetric. If ξ is reduced, then Theorem 1.3.5 implies $a, b \in \mathbb{N}$. Conversely, if $a, b \in \mathbb{N}$, then $b^2 < 4a^2 + b^2 = \Delta < (b + 2a)^2$ and $(2a - b)^2 < \Delta$. Hence it follows that $0 < \sqrt{\Delta} - b < 2a < \sqrt{\Delta} + b$, and therefore ξ is reduced.

2. (a) $\Leftrightarrow$ (b) Since $\xi + \xi' = \mathcal{T}(\xi) = a^{-1}b$, it follows that ξ is ambiguous if and only if $\xi + \xi' \in \mathbb{Z}$.

(b) $\Leftrightarrow$ (c) Obvious, since $\xi' + (\xi^\#)^{-1} = \xi' + \xi - \lfloor \xi \rfloor$.

If $\xi^\# = -\xi'^{-1}$, then ξ is ambiguous by (c). Assume now that ξ is ambiguous and reduced. Then $\xi^\#$ is also reduced, hence $(\xi^\#)^{-1} \in (0, 1)$, $\xi' \in (-1, 0)$, and since $\xi' + (\xi^\#)^{-1} \in \mathbb{Z}$, it follows that $\xi' + (\xi^\#)^{-1} = 0$ and $\xi^\# = -\xi'^{-1}$.

3. If ξ is ambiguous, then $\xi' = -\xi + n \sim \xi$ for some $n \in \mathbb{Z}$, and if ξ is symmetric, then $\xi = -\xi'^{-1} \sim \xi'$. Hence ξ is weakly ambiguous in either case.

If ξ is weakly ambiguous, then $\xi^\# \sim \xi$ implies $(\xi^\#)' \sim \xi' \sim \xi \sim \xi^\#$, and thus $\xi^\#$ is also weakly ambiguous. □

In the following Theorem 2.3.3 we determine the structure of inverse periods. This result, due to Galois, is the main tool in the subsequent investigations of the periods of weakly ambiguous quadratic irrationals.

Theorem 2.3.3 (Inverse periods)**.** *Let $\Delta > 0$ be a quadratic discriminant and ξ a reduced quadratic irrational of discriminant Δ. Let $l = l(\xi)$ be the period length, $(\xi_0, \xi_1, \ldots, \xi_{l-1})$ the period and $\xi = [u_0, u_1, \ldots] = [\,\overline{u_0, \ldots, u_{l-1}}\,]$ the continued fraction of $\xi = \xi_0$. Then l is also the period length of $-\xi'^{-1}$,*

$$-\xi'^{-1} = [\,\overline{u_{l-1}, u_{l-2}, \ldots, u_0}\,] \quad \textit{and} \quad \mathsf{z}(-\xi'^{-1}) = (-\xi_0'^{-1}, -\xi_{l-1}'^{-1}, \ldots, -\xi_1'^{-1})\,.$$

In particular, if $(\xi_n)_{n\in\mathbb{Z}}$ is the periodic extension of $\mathsf{z}(\xi)$ and $(\xi_n^*)_{n\in\mathbb{Z}}$ is the periodic extension of $\mathsf{z}(-\xi'^{-1})$, then $\xi_n^* = -\xi_{-n}'^{-1}$ for all $n \in \mathbb{Z}$.

Proof. By Theorem 1.3.5.2, $-\xi'^{-1}$ is a reduced quadratic irrational of discriminant Δ. We assert that it suffices to prove the following assertion:

A. For all $i \in [0, l]$ we have $-\xi'^{-1} = [u_{l-1}, u_{l-2}, \ldots, u_{l-i}, -\xi_{l-i}'^{-1}]$.

Indeed, for $i = l$, **A** implies $-\xi'^{-1} = [u_{l-1}, u_{l-2} \ldots, u_0, -\xi'^{-1}]$, and therefore

$$-\xi'^{-1} = [\,\overline{u_{l-1}, u_{l-2}, \ldots, u_0}\,]\,.$$

Hence $l(-\xi'^{-1}) = l$, and if $\mathsf{z}(-\xi'^{-1}) = (\xi_0^*, \ldots, \xi_{l-1}^*)$ is the period of $-\xi'^{-1}$, then

$$\begin{aligned}\xi_\mu^* &= [\,\overline{u_{l-\mu-1}, u_{l-\mu-2}, \ldots, u_0, u_{l-1}, \ldots, u_{l-\mu}}\,]\\ &= -\xi_{l-\mu}'^{-1} \quad \text{for all} \quad \mu \in [0, l-1]\,.\end{aligned}$$

By periodicity we obtain $\xi_n^* = -\xi_{l-n}'^{-1} = -\xi_{-n}'^{-1}$ for all $n \in \mathbb{Z}$.

Proof of **A**. We proceed by induction on i.

$i = 0$: Obvious, since $\xi_l = \xi_0 = \xi$.

$i \in [0, l-1]\,,\ i \to i+1$: Since $\xi_{l-i-1} = u_{l-i-1} + \xi_{l-i}^{-1}$, it follows that

$$\xi_{l-i-1}' = u_{l-i-1} + \frac{1}{\xi_{l-i}'}\,, \qquad -\xi_{l-i}' = u_{l-i-1} + \frac{1}{-\xi_{l-i-1}'}\,,$$

and by the induction hypothesis we obtain

$$-\xi'^{-1} = \Bigl[u_{l-1}, \ldots, u_{l-i}, u_{l-i-1} + \frac{1}{-\xi_{l-i-1}'}\Bigr] = [u_{l-1}, \ldots, u_{l-i}, u_{l-i-1}, -\xi_{l-i-1}']\,. \qquad \square$$

Theorem 2.3.4 (Periods of weakly ambiguous quadratic irrationals)**.** *Let ξ be a weakly ambiguous quadratic irrational of discriminant $\Delta > 0$, l its period length, $\mathsf{z} = (\xi_0, \xi_1, \ldots, \xi_{l-1})$ its period and $(\xi_i)_{i\in\mathbb{Z}}$ its periodic extension. Then there exists a unique index $n \in [0, l-1]$ such that $-\xi_0'^{-1} = \xi_n$.*

- *If $l = 2k$ for some $k \in \mathbb{N}$, then either z contains two ambiguous and no symmetric numbers, or z contains two symmetric and no ambiguous numbers. If $q \in \mathbb{Z}$ and ξ_q is ambiguous [symmetric], then ξ_{q+k} is ambiguous [symmetric], too.*

- *If* $l = 2k-1$ *for some* $k \in \mathbb{N}$*, then* z *contains precisely one ambiguous and one symmetric number (which coincide if* $l=1$ *). If* $q \in \mathbb{Z}$ *and* ξ_q *is ambiguous, then* ξ_{q+k} *is symmetric, and if* ξ_q *is symmetric, then* ξ_{q+k-1} *is ambiguous.*

The distribution of ambiguous and symmetric numbers in the period subject to n *is given by the following table:*

l	n	ambiguous numbers	symmetric numbers
$2k$	$2m+1$	$\xi_m,\ \ \xi_{m+k}$	–
$2k$	$2m$	–	$\xi_m,\ \ \xi_{m+k}$
$2k-1$	$2m+1$	ξ_m	ξ_{m+k}
$2k-1,$	$2m$	ξ_{m+k-1}	ξ_m

The number $n = \mathsf{p}(\xi_0)$ is called the *palindromic index* of the reduced weakly ambiguous quadratic irrational ξ_0. In terms of ideals, it was introduced by R. Mollin to study ambiguous ideal classes without ambiguous ideals (see [**73**] and [**74**, Ch. 6]). We shall return to this subject in Section 5.5.

Proof. We set $l = 2k-e$, where $k \in \mathbb{N}$ and $e \in \{0,1\}$. Since $\xi \sim \xi_0$, it follows that ξ_0 is weakly ambiguous, and therefore $\xi_0 \sim \xi_0' \sim -\xi_0'^{-1}$. Since $-\xi_0'^{-1}$ is reduced, there exists a unique index $n \in [0, l-1]$ such that $-\xi_0'^{-1} = \xi_n$, hence $\mathsf{z}(-\xi_0'^{-1}) = (\xi_n, \xi_{n+1}, \ldots, \xi_{n+l-1})$, and Theorem 2.3.3 implies $\xi_{n+j} = -\xi_{-j}'^{-1}$ for all $j \in \mathbb{Z}$.

CASE 1: $n = 2m+1$ for some $m \in \mathbb{N}_0$. Then $\xi_{m+1} = \xi_{n-m} = -\xi_m'^{-1}$, and thus ξ_m is ambiguous. Since $\xi_{m+k+1-e} = \xi_{n-m+k-e} = -\xi_{m-k+e}'^{-1} = -\xi_{m+k}'^{-1}$, it follows that ξ_{m+k} is symmetric if $e=1$, and ξ_{m+k} is ambiguous if $e=0$.

CASE 2: $n = 2m$ for some $m \in \mathbb{N}$. Then $\xi_m = \xi_{n-m} = -\xi_m'^{-1}$, and thus ξ_m is symmetric. Since $\xi_{m+k} = \xi_{n-m+k} = -\xi_{m-k}'^{-1} = -\xi_{m+k-e}'^{-1}$, it follows that ξ_{m+k} is symmetric if $e=0$, and ξ_{m+k-1} is ambiguous if $e=1$.

Up to now we have proved: If $e=1$, then z contains one symmetric and one ambiguous number, and if $e=0$, then z contains either two symmetric or two ambiguous numbers. Therefore it remains to prove the following two assertions:

a. If $q \in \mathbb{Z}$ and $h \in [1, l-1]$ are such that ξ_q is ambiguous and ξ_{q+h} is symmetric, then $l = 2h-1$.

b. If $q \in \mathbb{Z}$ and $h \in [1, l-1]$ are such that both ξ_q and ξ_{q+h} are either ambiguous or symmetric, then $l = 2h$.

a. Let $q \in \mathbb{Z}$ and $h \in [1, l-1]$ be such that ξ_q is ambiguous and ξ_{q+h} is symmetric. Then $\xi_{q+1} = -\xi_q'^{-1}$ and $\xi_{q+h} = -\xi_{q+h}'^{-1}$, which implies $\xi_{q+h+j} = -\xi_{q+h-j}'^{-1}$ for all $j \in \mathbb{Z}$. For $j = h$ we obtain $\xi_{q+2h} = -\xi_q'^{-1} = \xi_{q+1}$ and consequently $l = 2h-1$.

b$_1$. Let $q \in \mathbb{Z}$ and $h \in [1, l-1]$ be such that ξ_q and ξ_{q+h} are both ambiguous. Then $\xi_{q+1} = -\xi_q'^{-1}$ and $\xi_{q+h+1} = -\xi_{q+h}'^{-1}$, which implies $\xi_{q+h+1+j} = -\xi_{q+h-j}'^{-1}$ for all $j \in \mathbb{Z}$. For $j = h$ we obtain $\xi_{q+2h+1} = -\xi_q'^{-1} = \xi_{q+1}$ and consequently $l = 2h$.

b$_2$. Let $q \in \mathbb{Z}$ and $h \in [1, l-1]$ be such that ξ_q and ξ_{q+h} are both symmetric. Then $\xi_q = -\xi_q'^{-1}$ and $\xi_{q+h} = -\xi_{q+h}'^{-1}$, which implies $\xi_{q+h+j} = -\xi_{q+h-j}'^{-1}$ for all $j \in \mathbb{Z}$. For $j = h$ we obtain $\xi_{q+2h} = -\xi_q'^{-1} = \xi_q$ and consequently $l = 2h$. $\square$

We close this chapter with a thorough investigation of the continued fraction of the basis number ω_Δ associated with a quadratic discriminant $\Delta > 0$.

The case $\Delta = 5$ is special. Indeed,

$$\varepsilon_5 = \omega_5 = \frac{1+\sqrt{5}}{2} = 1 + \frac{1}{\omega_5}\,, \quad \text{hence} \quad \omega_5^\# = \omega_5 \quad \text{and} \quad \omega_5 = [1, 1, \ldots] = [\,\overline{1}\,]\,.$$

Consequently, ω_5 is reduced, ambiguous and symmetric, and $l(\omega_5) = 1$. Let $(p_n)_{n \ge -2}$ be the sequence of partial numerators and $(q_n)_{n \ge -2}$ the sequence of partial denominators of ω_5. Then $p_{n-2} = q_{n-1} = F_n$ for all $n \ge 0$, where $(F_n)_{n \ge 0}$ denotes the Fibonacci sequence, defined by $F_0 = 0,\ F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for all $n \ge 2$ (see Exercise 2.1.5).

The following voluminous Theorem 2.3.5 contains detailed information about the continued fraction of the basis numbers ω_Δ for $\Delta > 5$.

Theorem 2.3.5. *Let $\Delta > 5$ be a quadratic discriminant and $\Delta = 4D + \sigma$, where $D \in \mathbb{N}$ and $\sigma \in \{0, 1\}$. Let $\omega_\Delta = [u_0, u_1, \ldots]$ be the continued fraction and l the period length of ω_Δ. Then $u_l = 2u_0 - \sigma \ne u_0,\ u_{l-i} = u_i$ for all $i \in [1, l-1]$, and*

$$\omega_\Delta = \frac{\sigma + \sqrt{\Delta}}{2} = [u_0, \overline{u_1, u_2, \ldots, u_2, u_1, 2u_0 - \sigma}\,]\,.$$

Let $(p_n)_{n \ge -2}$ be the sequence of partial numerators, $(q_n)_{n \ge -2}$ the sequence of partial denominators and $(\xi_n)_{n \ge 0}$ the sequence of complete quotients of ω_Δ. If $n \ge 0$ and ξ_n is of type (a_n, b_n, c_n), then $a_n \ge 1,\ \ b_n = 2B_n - \sigma$ with $B_n \in \mathbb{Z},\ \ a_0 = 1$, $b_0 = B_0 = \sigma$, the number

$$\xi_l = [\,\overline{2u_0 - \sigma, u_1, u_2, \ldots, u_2, u_1}\,] = u_0 - \omega_\Delta' = \frac{2u_0 - \sigma + \sqrt{\Delta}}{2}$$

is ambiguous and reduced, $a_l = 1$ and $B_l = u_0$.

1. *For all $n \ge 0$, the following relations hold:*
   (a) *$B_{n+1} = -B_n + a_n u_n + \sigma$ and $a_n a_{n+1} = D - B_{n+1}(B_{n+1} - \sigma)$.*
   (b) *$p_{n-1} = B_n q_{n-1} + a_n q_{n-2}$.*
   (c) *$D q_{n-1} = (B_n - \sigma) p_{n-1} + a_n p_{n-2}$.*
   (d) *$4(-1)^n a_n = (2p_{n-1} - \sigma q_{n-1})^2 - \Delta q_{n-1}^2 = 4\mathcal{N}(p_{n-1} - q_{n-1}\omega_\Delta)$.*
   (e) *$(-1)^n a_n = p_{n-1}^2 - \sigma p_{n-1} q_{n-1} - D q_{n-1}^2$.*
2. *$B_{i+1} = B_{l-i}$ for all $i \in [0, l-1]$, and $a_i = a_{l-i}$ for all $i \in [0, l]$.*
3. *If $i \ge -1$ and $n \ge 0$, then*
$$p_{i+nl} - q_{i+nl}\omega_\Delta = (p_i - q_i\omega_\Delta)(p_{l-1} - q_{l-1}\omega_\Delta)^n\,.$$
4. *If ε_Δ is the fundamental unit of discriminant Δ, then $\mathcal{N}(\varepsilon_\Delta) = (-1)^l$, and*
$$\varepsilon_\Delta^m = (p_{l-1} - q_{l-1}\omega_\Delta')^m = p_{ml-1} - q_{ml-1}\omega_\Delta' \quad \textit{for all} \ \ m \ge 0\,.$$
5. *Suppose that $k \in [0, l-1]$. Then $a_{k+1} = a_k$ if and only if $l = 2k+1$. In this case, ξ_l is the only ambiguous number in the period of ω_Δ, and ξ_{k+1} is symmetric.*

6. *Suppose that* $k \in [1, l-1]$. *Then* $B_{k+1} = B_k$ *if and only if* $l = 2k$. *In this case,* ξ_l *and* ξ_k *are the only ambiguous numbers in the period of* ω_Δ, $2B_k = a_k u_k + \sigma$, *and the following assertions hold*:
   (a) $2p_{k-1} - \sigma q_{k-1} = a_k(q_k + q_{k-2})$.
   (b) $q_{l-1} = q_{k-1}(q_k + q_{k-2})$.
   (c) $a_k p_{l-1} = p_{k-1}^2 + Dq_{k-1}^2$.
   (d) $(p_{k-1} - q_{k-1}\omega'_\Delta)^2 = a_k\, \varepsilon_\Delta$.

Proof. By definition, $\omega_\Delta > 1$, $u_0 = \lfloor \omega_\Delta \rfloor \geq 2$, $\omega_\Delta^\# = (\omega_\Delta - u_0)^{-1} > 1$, and $(\omega_\Delta^\#)' = (\omega'_\Delta - u_0)^{-1} = (-\omega_\Delta + \sigma - u_0)^{-1} \in (-1, 0)$. Hence $\omega_\Delta^\#$ is reduced, and therefore $\omega_\Delta^\# = [\,\overline{u_1, \ldots, u_l}\,]$, where $l = l(\omega_\Delta)$, and Theorem 2.3.3 implies that $-(\omega_\Delta^\#)'^{-1} = [\,\overline{u_l, u_{l-1}, \ldots, u_1}\,]$. On the other hand,

$$-(\omega_\Delta^\#)'^{-1} = u_0 - \sigma + \omega_\Delta = [2u_0 - \sigma, u_1, u_2, \ldots\,],$$

and by the uniqueness of the continued fraction it follows that $u_l = 2u_0 - \sigma \neq u_0$ and $u_{l-i} = u_i$ for all $i \in [1, l-1]$. In particular, the number

$$\xi_l = [\,\overline{u_l, u_1, \ldots, u_{l-1}}\,] = [\,2u_0 - \sigma, \overline{u_1, \ldots, u_l}\,] = u_0 - \sigma + \omega_\Delta = u_0 - \omega'_\Delta$$

is reduced, and as it is of type $(1, 2u_0 - \sigma, u_0^2 - u_0\sigma - D)$, it is ambiguous.

Assume now that $n \geq 0$, let ξ_n be of type (a_n, b_n, c_n), and apply Theorem 2.2.6 again and again. By definition, $a_0 = 1$, and if $n \geq 1$, then $a_n \geq 1$ since ξ_n is reduced. As $b_n + b_{n+1} = 2a_n u_n \equiv 0 \bmod 2$ and $b_0 = \sigma$, it follows by a simple induction that $b_n \equiv \sigma \bmod 2$, and thus $b_n = 2B_n - \sigma$ for some $B_n \in \mathbb{Z}$.

1. (a) $2a_n u_n = b_n + b_{n+1} = 2B_n + 2B_{n+1} - 2\sigma$, hence $B_{n+1} = -B_n + a_n u_n + \sigma$, and $4a_n a_{n+1} = \Delta - b_{n+1}^2 = 4D + \sigma - (2B_{n+1} - \sigma)^2 = 4(D - B_{n+1}^2 + \sigma B_{n+1})$, hence $a_n a_{n+1} = D - B_{n+1}(B_{n+1} - \sigma)$.

(b) Since $a_0 = 1$ and $b_0 = \sigma$, we obtain

$$2p_{n-1} - \sigma q_{n-1} = b_n q_{n-1} + 2a_n q_{n-2} = (2B_n - \sigma)q_{n-1} + 2a_n q_{n-2},$$

and therefore $p_{n-1} = B_n q_{n-1} + a_n q_{n-2}$.

(c) Since $\Delta = 4D + \sigma$ and $b_n = 2B_n - \sigma$, we obtain

$$\begin{aligned}(4D + \sigma)q_{n-1} &= 2\,[\,p_{n-1}(2B_n - \sigma) + 2p_{n-2}a_n] - \sigma\,[\,q_{n-1}(2B_n - \sigma) + 2q_{n-2}a_n] \\ &= 4B_n p_{n-1} + 4a_n p_{n-2} + \sigma q_{n-1} - 2\sigma(p_{n-1} + B_n q_{n-1} + a_n q_{n-2}).\end{aligned}$$

By (b), it follows that $p_{n-1} + B_n q_{n-1} + a_n q_{n-2} = 2p_{n-1}$, and therefore we get $Dq_{n-1} = (B_n - \sigma_\Delta)p_{n-1} + a_n p_{n-2}$.

(d) and (e) Obvious by Theorem 2.2.6.1(g).

2. We have already seen that $a_0 = a_l = 1$. Thus suppose that $i \in [0, l-1]$. Then $\xi_{i+1} = [\,\overline{u_{i+1}, \ldots, u_l, u_1, \ldots, u_i}\,]$, and therefore

$$-\xi_{i+1}'^{-1} = [\,\overline{u_i, \ldots, u_1, u_l, \ldots, u_{i+1}}\,] = [\,\overline{u_{l-i}, \ldots, u_{l-1}, u_l, u_1, \ldots, u_{l-i-1}}\,] = \xi_{l-i}.$$

$-\xi_{i+1}'^{-1}$ is of type $(-c_{i+1}, b_{i+1}, -a_{i+1}) = (a_i, b_{i+1}, -a_{i+1})$, and since ξ_{l-i} is of type $(a_{l-i}, b_{l-i}, c_{l-i})$, it follows that $a_i = a_{l-i}$ and $b_{i+1} = b_{l-i}$, hence $B_{i+1} = B_{l-i}$.

3. Suppose that $i \ge -1$ and proceed by induction on n. For $n = 0$, there is nothing to do.

$n \ge 1,\ n-1 \to n$: We set $j = i + (n-1)l$. Then the induction hypothesis implies $p_j - q_j\omega_\Delta = (p_i - q_i\omega_\Delta)(p_{l-1} - q_{l-1}\omega_\Delta)^{n-1}$, and thus it suffices to prove that

$$p_{l+j} - q_{l+j}\omega_\Delta = (p_j - q_j\omega_\Delta)(p_{l-1} - q_{l-1}\omega_\Delta)\,.$$

Since $(1, \omega_\Delta)$ is linearly independent and

$$\begin{aligned}(p_j - q_j\omega_\Delta)(p_{l-1} - q_{l-1}\omega_\Delta) &= p_jp_{l-1} - (p_jq_{l-1} + q_jp_{l-1})\omega_\Delta + q_jq_{l-1}(D + \sigma\omega_\Delta) \\ &= p_jp_{l-1} + q_jq_{l-1}D + (q_jq_{l-1}\sigma - p_jq_{l-1} - q_jp_{l-1})\omega_\Delta\,,\end{aligned}$$

we must prove that

$$p_{j+l} = p_jp_{l-1} + q_jq_{l-1}D \quad \text{and} \quad q_{j+l} = p_jq_{l-1} + q_jp_{l-1} - \sigma q_jq_{l-1}\,.$$

From the matrix equation

$$\begin{aligned}\begin{pmatrix} p_{j+l} & p_{j+l-1} \\ q_{j+l} & q_{j+l-1}\end{pmatrix} &= \prod_{\nu=0}^{l+j}\begin{pmatrix} u_\nu & 1 \\ 1 & 0\end{pmatrix} = \begin{pmatrix} p_l & p_{l-1} \\ q_l & q_{l-1}\end{pmatrix}\prod_{\nu=l+1}^{l+j}\begin{pmatrix} u_\nu & 1 \\ 1 & 0\end{pmatrix} \\ &= \begin{pmatrix} p_l & p_{l-1} \\ q_l & q_{l-1}\end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -u_0\end{pmatrix}\prod_{\nu=0}^{j}\begin{pmatrix} u_\nu & 1 \\ 1 & 0\end{pmatrix} = \begin{pmatrix} p_{l-1} & p_l - u_0p_{l-1} \\ q_{l-1} & q_l - u_0q_{l-1}\end{pmatrix}\begin{pmatrix} p_j & p_{j-1} \\ q_j & q_{j-1}\end{pmatrix}\end{aligned}$$

it follows that

$$p_{j+l} = p_jp_{l-1} + (p_l - u_0p_{l-1})q_j \quad \text{and} \quad q_{j+l} = p_jq_{l-1} + (q_l - u_0q_{l-1})q_j\,.$$

Since $u_l - u_0 = B_l - \sigma$ and $a_l = 1$, we obtain, using 1.(c) and 1.(b),

$$p_l - u_0p_{l-1} = u_lp_{l-1} + p_{l-2} - u_0p_{l-1} = (B_l - \sigma)p_{l-1} + a_lp_{l-2} = q_{l-1}D$$

and

$$q_l - u_0q_{l-1} = u_lq_{l-1} + q_{l-2} - u_0q_{l-1} = (B_l - \sigma)q_{l-1} + a_lq_{l-2} = p_{l-1} - \sigma q_{l-1}\,.$$

Now the assertion follows.

4. By Theorem 2.2.6.2, Theorem 2.2.9 and 3., we obtain

$$\begin{aligned}\varepsilon_\Delta^m &= \prod_{i=1}^{ml}\xi_i = (-1)^{ml}(p_{ml-1} - q_{ml-1}\omega_\Delta)^{-1} = \frac{(-1)^{ml}(p_{ml-1} - q_{ml-1}\omega_\Delta')}{\mathcal{N}(p_{ml-1} - q_{ml-1}\omega_\Delta)} \\ &= \frac{(p_{ml-1} - q_{ml-1}\omega_\Delta')a_0}{a_{ml}} = p_{ml-1} - q_{ml-1}\omega_\Delta' = (p_{l-1} - q_{l-1}\omega_\Delta')^m\end{aligned}$$

and $\mathcal{N}(\varepsilon_\Delta^m) = (-1)^{ml}$.

5. Suppose that $k \in [0, l-1]$. If $l = 2k+1$, then $a_{k+1} = a_{l-k-1} = a_k$. Conversely, if $a_{k+1} = a_k$, then 2. implies

$$\xi_{k+1} = \frac{b_{k+1} + \sqrt{\Delta}}{2a_{k+1}} = \frac{b_{k+1} + \sqrt{\Delta}}{2a_k} = \frac{b_{l-k} + \sqrt{\Delta}}{2a_{l-k}} = \xi_{l-k}\,,$$

and since $\xi_0, \xi_1, \ldots, \xi_l$ are distinct, we obtain $k+1 = l-k$ and $l = 2k+1$. By Theorem 2.3.4.1, ξ_l is the only ambiguous number in the period $(\xi_1, \ldots, \xi_l)$ of ω_Δ, and $\xi_{l+k+1} = \xi_{k+1}$ is symmetric.

6. Suppose that $k \in [0, l-1]$. If $l = 2k$, then $B_{k+1} = B_{l-k} = B_k$, and therefore $2B_k = a_k u_k + \sigma$ by 1. (a). Conversely, if $B_{k+1} = B_k$, then $b_{k+1} = b_k$, and 2. implies

$$\xi_k = \frac{b_k + \sqrt{\Delta}}{2a_k} = \frac{b_{k+1} + \sqrt{\Delta}}{2a_k} = \frac{b_{l-k} + \sqrt{\Delta}}{2a_{l-k}} = \xi_{l-k}\,.$$

Since $\xi_0, \xi_1, \ldots, \xi_l$ are distinct, we obtain $l - k = k$, hence $l = 2k$, and Theorem 2.3.4.2 implies that ξ_l and $\xi_{l+k} = \xi_k$ are the only ambiguous numbers in the period $(\xi_1, \ldots, \xi_l)$ of ω_Δ.

(a) Using 1.(b), we obtain

$$\begin{aligned} 2p_{k-1} - \sigma q_{k-1} &= 2B_k q_{k-1} + 2a_k q_{k-2} - \sigma q_{k-1} = a_k u_k q_{k-1} + 2a_k q_{k-2} \\ &= a_k(q_k + q_{k-2})\,. \end{aligned}$$

(b), (c) From the matrix equation

$$\begin{aligned} \begin{pmatrix} p_{l-1} & p_{l-2} \\ q_{l-l} & q_{l-2} \end{pmatrix} &= \prod_{\nu=0}^{l-1} \begin{pmatrix} u_\nu & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_{k-1} & p_{k-2} \\ q_{k-1} & q_{k-2} \end{pmatrix} \prod_{\nu=k}^{l-1} \begin{pmatrix} u_\nu & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} p_{k-1} & p_{k-2} \\ q_{k-1} & q_{k-2} \end{pmatrix} \prod_{\nu=k}^{l-1} \begin{pmatrix} u_{l-\nu} & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} p_{k-1} & p_{k-2} \\ q_{k-1} & q_{k-2} \end{pmatrix} \left[\prod_{\nu=0}^{k} \begin{pmatrix} u_\nu & 1 \\ 1 & 0 \end{pmatrix} \right]^{\mathsf{t}} \begin{pmatrix} 0 & 1 \\ 1 & -u_0 \end{pmatrix} \\ &= \begin{pmatrix} p_{k-1} & p_{k-2} \\ q_{k-1} & q_{k-2} \end{pmatrix} \begin{pmatrix} p_k & q_k \\ p_{k-1} & q_{k-1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -u_0 \end{pmatrix} \\ &= \begin{pmatrix} p_{k-1} & p_{k-2} \\ q_{k-1} & q_{k-2} \end{pmatrix} \begin{pmatrix} q_k & p_k - u_0 q_k \\ q_{k-1} & p_{k-1} - u_0 q_{k-1} \end{pmatrix} \end{aligned}$$

it follows that $p_{l-1} = p_{k-1}q_k + p_{k-2}q_{k-1}$ and $q_{l-1} = q_{k-1}(q_k + q_{k-2})$. By 1.(c), we get

$$\begin{aligned} a_k p_{l-1} &= a_k p_{k-1} q_k + a_k p_{k-2} q_{k-1} \\ &= a_k p_{k-1} q_k + D q_{k-1}^2 - (B_k - \sigma) p_{k-1} q_{k-1} \\ &= p_{k-1}[\, a_k u_k q_{k-1} + a_k q_{k-2} - (B_k - \sigma) q_{k-1}] + D q_{k-1}^2 \\ &= p_{k-1}(B_k q_{k-1} + a_k q_{k-2}) + D q_{k-1}^2 = p_{k-1}^2 + D q_{k-1}^2\,. \end{aligned}$$

(d) Using (a), (b) and (c), we obtain

$$\begin{aligned} (p_{k-1} - q_{k-1}\omega'_\Delta)^2 &= (p_{k-1}^2 + D q_{k-1}^2) - q_{k-1}(2p_{k-1} - \sigma q_{k-1})\omega'_\Delta \\ &= a_k p_{l-1} + a_k q_{k-1}(q_k + q_{k-2})\omega'_\Delta \\ &= a_k(p_{l-1} + q_{l-1}\omega'_\Delta) = a_k \varepsilon_\Delta\,, \end{aligned}$$

which completes the proof. □

In the following Examples 2.3.6, 2.3.7 and 2.3.8, we apply our theory to calculate the continued fraction of the basis number and the fundamental unit for some special quadratic discriminants.

Example 2.3.6. Let $\Delta = 4a^2 + r$ be a quadratic discriminant, where $a,\, r \in \mathbb{N}$, $r \equiv 1 \bmod 4$ and $r \,|\, a$. We start with $\xi_0 = \omega_\Delta,\ \ \sigma = 1,\ \ B_0 = a_0 = 1,\ \ \Delta = 4D + 1$, and for $n \ge 0$ we use the formulas $u_n = \lfloor \xi_n \rfloor,\ \ B_{n+1} = -B_n + a_n u_n + 1$,

$$\xi_n = \frac{2B_n - 1 + \sqrt{\Delta}}{2a_n} \quad \text{and} \quad a_{n+1} = \frac{D - B_{n+1}(B_{n+1} - 1)}{a_n}\,.$$

We obtain the following table.

n	B_n	a_n	ξ_n	u_n	p_n	q_n
0	1	1	$\frac{1+\sqrt{\Delta}}{2}$	a	a	1
1	a	$a + \frac{r-1}{4}$	$\frac{4a-2+\sqrt{\Delta}}{4a+r-1}$	1	$a+1$	1
2	$\frac{r+3}{4}$	$a - \frac{r-1}{4}$	$\frac{r+1+2\sqrt{\Delta}}{4a-r+1}$	1	$2a+1$	2
3	$a - \frac{r-1}{2}$	r	$\frac{2a-r+\sqrt{\Delta}}{2r}$	$\frac{2a}{r} - 1$		
4	$a - \frac{r-1}{2}$					

Since $B_3 = B_4$, we get $k = 3,\ \ l(\omega_\Delta) = 6$, and $a_3\varepsilon_\Delta = (p_2 - q_2\omega'_\Delta)^2$, which implies

$$\varepsilon_\Delta = \frac{(2a + \sqrt{\Delta})^2}{r} = \frac{8a^2}{r} + 1 + \frac{4a}{r}\sqrt{4a^2 + r} \quad \text{and} \quad \mathcal{N}(\varepsilon_\Delta) = 1\,.$$

Example 2.3.7. Let $\Delta = 4D$ be a quadratic discriminant, where $D = a^2 - r$ for some $a,\, r \in \mathbb{N},\ \ a \ge 3,\ \ r \,|\, 2a$ and $r < 2a$. We start with $\xi_0 = \sqrt{D},\ \ \sigma = B_0 = 0$, $a_0 = 1$, and for $n \ge 0$ we use the formulas $u_n = \lfloor \xi_n \rfloor,\ \ B_{n+1} = -B_n + a_n u_n$,

$$\xi_n = \frac{B_n + \sqrt{D}}{a_n} \quad \text{and} \quad a_{n+1} = \frac{D - B_{n+1}^2}{a_n}\,.$$

We obtain the following table.

n	B_n	a_n	ξ_n	u_n	p_n	q_n
0	0	1	$\sqrt{D}$	$a-1$	$a-1$	1
1	$a-1$	$2a-r-1$	$\frac{a-1+\sqrt{D}}{2a-r-1}$	1	a	1
2	$a-r$	r	$\frac{a-r+\sqrt{D}}{2a-r-1}$	$\frac{2a}{r} - 2$		
3	$a-r$					

Since $B_2 = B_3$, we get $k = 2,\ \ l(\sqrt{D}) = 4$, and $a_2\varepsilon_\Delta = (p_1 + q_1\sqrt{D})^2$, which implies

$$\varepsilon_\Delta = \frac{(a + \sqrt{D})^2}{r} = \frac{2a^2}{r} - 1 + \frac{2a}{r}\sqrt{a^2 - r} \quad \text{and} \quad \mathcal{N}(\varepsilon_\Delta) = 1\,.$$

In the previous two examples we considered positive quadratic discriminants Δ of the so-called *extended Richaud-Degert type* (that means, $D = a^2 + r$, where $a \in \mathbb{N},\ \ r \in \mathbb{Z},\ \ r \,|\, 4a$, and either $\Delta = D \equiv 1 \bmod 4$ or $\Delta = 4D$). A thorough study of these discriminants (not only in the context of continued fractions, but also in connection with Diophantine equations and class numbers) can be found in Mollin's book [**74**]. We present one further Richaud-Degert discriminant which seems not to be treated in [**75**] and leave some others as exercises.

Example 2.3.8. Let $\Delta = 4D$ be a quadratic discriminant, where $D = a^2 - 4a$ for some odd integer $a \geq 7$. We start with $\xi_0 = \sqrt{D}$, $\sigma = B_0 = 0$, $a_0 = 1$, and for $n \geq 0$ we use the same formulas as in Example 2.3.7. We obtain the following table.

n	B_n	a_n	ξ_n	u_n	p_n	q_n
0	0	1	$\sqrt{D}$	$a-3$	$a-3$	1
1	$a-3$	$2a-9$	$\frac{a-3+\sqrt{D}}{2a-9}$	1	$a-2$	1
2	$a-6$	4	$\frac{a-6+\sqrt{D}}{4}$	$\frac{a-5}{2}$	$\frac{a^2-5a+4}{2}$	$\frac{a-3}{2}$
3	$a-4$	$a-4$	$\frac{a-4+\sqrt{D}}{a-4}$	2		
4	$a-4$					

Since $B_3 = B_4$, we get $k = 3$, $l(\sqrt{D}) = 6$, and $a_3\varepsilon_\Delta = (p_2 + q_2\sqrt{D})^2$, which implies

$$\varepsilon_\Delta = \frac{a^3 - 6a^2 + 9a - 2}{2} + \frac{a^2 - 4a + 3}{2}\sqrt{a^2 - 4a} \quad \text{and} \quad \mathcal{N}(\varepsilon_\Delta) = 1\,.$$

Exercise 2.3.9. Calculate the continued fraction of ω_Δ and the fundamental unit ε_Δ for the following quadratic discriminants:

a) $\Delta = 4D$, where $D = a^2 + r$ for some $a,\ r \in \mathbb{N}$ such that $a \geq 3$ and $r \mid 2a$.

b) $\Delta = a^2 + 4r$, where $a \in \mathbb{N}$ is odd, $r \in \mathbb{N}$, $r \mid a$ and $r < a$.

A famous widely open conjecture of Gauss states that there are infinitely many primes $p \equiv 1 \bmod 4$ satisfying $h_p = 1$. A weaker form of this conjecture asserts that for some integer $B > 1$ there exist infinitely many fundamental discriminants Δ such that $h_\Delta < B$, but even this weaker conjecture is at present out of reach. If we allow non-fundamental discriminants, a construction using Fibonacci numbers in Section 5.7 will show that $h_{5^{2n+1}} = 1$ for all $n \in \mathbb{N}$.

By a theorem of Siegel,

$$h_\Delta \log \varepsilon_\Delta = \Delta^{1/2+\delta_\Delta}, \quad \text{where} \quad \lim_{\Delta \to \infty} \delta_\Delta = 0\,,$$

holds for fundamental discriminants $\Delta > 0$ (for a proof see [**43**, Ch. 12.15]). If Gauss' conjecture is true, then it follows that, for every $\delta \in \mathbb{R}_{>0}$, there exist infinitely many fundamental discriminants $\Delta > 0$ such that $\log \varepsilon_\Delta > \Delta^{1/2-\delta}$. Thus one possible approach towards Gauss' conjecture could be the construction of infinite sequences of fundamental discriminants with large fundamental units. The infinite series of quadratic discriminants Δ produced in the Examples 2.3.6, 2.3.7 and 2.3.8 all have $\log \varepsilon_\Delta \asymp \log \sqrt{\Delta}$, which means that there exist positive real numbers c_1, c_1 such that

$$c_1 \leq \frac{\log \varepsilon_\Delta}{\log \sqrt{\Delta}} \leq c_2 \quad \text{for all } \Delta \text{ in question, a very poor order of magnitude.}$$

If we want to construct infinite sequences of discriminants Δ with large fundamental units, we must achieve a large period length of ω_Δ. Indeed, if $(\xi_1, \ldots, \xi_l)$ is the period of ω_Δ and $l = l(\omega_\Delta)$ is its period length, then the Theorems 2.2.9 and 1.3.5 imply

$$\log \varepsilon_\Delta = \sum_{i=1}^{l} \log \xi_i < l(\omega_\Delta) \log \sqrt{\Delta}\,.$$

The best result hitherto is due to Y. Yamamoto [**113**] who proved that the quadratic discriminants $\Delta = (p^nq+p-1)^2+4p^nq$ (where p, q are primes and $q>p$) have fundamental units satisfying $\log\varepsilon_\Delta \gg (\log\sqrt{D})^3$, which means that there exists a positive real number c such that

$$\log\varepsilon_\Delta \ge c(\log\sqrt{D})^3 \quad \text{for all } \Delta \text{ in question.}$$

An improvement of Y. Yamamoto's result to $\log\varepsilon_\Delta \gg (\log\sqrt{D})^4$ announced in [**38**] turned out to be erroneous (see [**47**] for a slight improvement of Yamamoto's result in another direction).

There are many infinite series of quadratic discriminants $\Delta>0$ with known continued fractions having a period length of asymptotic magnitude $l(\omega_\Delta)\asymp\log\Delta$ and a fundamental unit ε_Δ satisfying $\log\varepsilon_\Delta\asymp(\log\sqrt{\Delta})^2$ (see [**89**], [**78**], [**111**] or [**37**] and the references given there). We give the details for the quadratic discriminants $\Delta=(2^n+3)^2-8$ (first introduced by D. Shanks [**98**] and then investigated by Y. Yamamoto [**113**]) and leave some similar series as exercises.

Example 2.3.10. Assume that $n\in\mathbb{N}$ and $\Delta=(2^n+3)^2-8=4D+1$, where

$$D=\frac{(2^n+3)^2-9}{4}\,.$$

We calculate the continued fraction of ω_Δ using the formulas stated in Example 2.3.6. We obtain

$$B_0=1\,,\quad a_0=1\,,\quad \xi_0=\omega_\Delta=\frac{1+\sqrt{\Delta}}{2}\quad\text{and}\quad u_0=2^{n-1}+1\,,$$

$$B_{2i-1}=2^{n-1}+1\,,\quad a_{2i-1}=2^{n-i+1}\,,\quad \xi_{2i-1}=\frac{2^n+1+\sqrt{\Delta}}{2^{n-i+2}}$$

$$\text{and}\quad u_{2i-1}=\begin{cases}2^{i-1} & \text{if}\quad i\le n\,,\\ 2^n+1 & \text{if}\quad i=n+1\end{cases}\qquad\text{for all } i\in[1,n+1]$$

$$B_{2i}=2^{n-1},\quad a_{2i}=2^i\,,\quad \xi_{2i}=\frac{2^n-1+\sqrt{\Delta}}{2^{i+1}}\quad\text{and}$$

$$u_{2i}=2^{n-i}\quad\text{for all } i\in[1,n].$$

Hence it follows that

$$\frac{1+\sqrt{\Delta}}{2}=\big[2^{n-1}+1,\,\overline{1,\,2^{n-1},\,2,\,2^{n-2},\,4,\ldots,2^{i-1},2^{n-i},\ldots,2^{n-1},1,\,2^n+1}\,\big]\,,$$

$l(\omega_\Delta)=2n+1$, and consequently $\mathcal{N}(\varepsilon_\Delta)=-1$. According to Theorem 2.2.9 we calculate

$$\varepsilon_\Delta=\prod_{j=1}^{2n+1}\xi_j=\prod_{i=1}^{n+1}\frac{2^n+1+\sqrt{\Delta}}{2^{n-i+2}}\prod_{i=1}^{n}\frac{2^n-1+\sqrt{\Delta}}{2^{i+1}}$$

$$=\frac{2^n+1+\sqrt{\Delta}}{2}\Big(\frac{2^n+3+\sqrt{\Delta}}{4}\Big)^n.$$

A simple calculation shows that

$$\lim_{n\to\infty}\frac{\log\varepsilon_\Delta}{(\log\sqrt{\Delta}\,)^2}=\frac{1}{\log 2}\,,\quad\text{and therefore}\quad \log\varepsilon_\Delta\asymp(\log\sqrt{\Delta}\,)^2\,.$$

Exercise 2.3.11. Assume that $n \geq 2$, and calculate the continued fraction of ω_Δ and the fundamental unit ε_Δ for the following discriminants:

a) $\Delta = (p^n q + p - 1)^2 + 4p^n q$, where $p,\ q \in \mathbb{N}$, $q \,|\, p-1$ and $\Delta \equiv 1 \bmod 4$.

b) $\Delta = 4D$, $D = (p^n q + c)^2 + p^n q$, where $p,\ q,\ c \in \mathbb{N}$, $p = 4c+1$ and $q \,|\, c$.

Distinguish in both cases between $q = 1$ and $q > 1$.

Exercise 2.3.12. For a quadratic discriminant $\Delta > 0$, let $c(\Delta)$ be the number of reduced quadratic irrationals of discriminant Δ. Prove that $h_\Delta \leq c(\Delta)$ and $h_\Delta \log \varepsilon_\Delta < c(\Delta) \log \sqrt{\Delta}$. Use Siegel's theorem mentioned above to prove that for every $B \in \mathbb{N}$ there are only finitely many positive fundamental discriminants Δ satisfying $c(\Delta) < B$.

The number $c(\Delta)$ is called the *caliber* of Δ (see [**63**], [**48**]).

This page intentionally left blank

CHAPTER 3

Quadratic residues and Gauss sums

This chapter is centered on quadratic reciprocity and the theory around it. In Section 3.1, we start with an elementary theory of power residues based on group-theoretic arguments. Then we specialize to quadratic residues. In Section 3.3, we prove Gauss' quadratic reciprocity law and (again) Fermat's theorem on sums of two squares. In our presentation, we disregard the historical development of the subject. For a readable appreciation of the historical development we refer the interested reader to the books [**107**] and [**67**]. In this volume, we use Gauss sums to give a concise proof of the quadratic reciprocity law, and we use Jacobi sums for a proof of the theorem on sums of two squares (compare to the presentations given in [**17**], [**44**] and, even more detailed, in [**6**]). Gauss and Jacobi sums are introduced in Section 3.2, and a thorough presentation of the theory of quadratic characters is given in Section 3.5. All this material however does not only permit a simple proof of the quadratic reciprocity law, but has wide influence on the development of the following chapters. It will be used for the theory of Dirichlet series in Chapter 4, for Gauss' genus theory of binary quadratic forms in Chapter 6, and for the theory of biquadratic residues in Chapter 7.

3.1. Elementary theory of power residues

Let m and $n \geq 2$ be positive integers. An integer a is called an *n-th power residue* modulo m if $a \equiv x^n \mod m$ for some $x \in \mathbb{Z}$. Otherwise we call a an *n-th power non-residue* modulo m. If $n = 2$ [$n = 3$, $n = 4$], then an n-th power (non-)residue modulo m is called a *quadratic* [*cubic, quartic or biquadratic*] (non-)residue modulo m.

From an algebraic point of view (which we shall adopt whenever this will be convenient) an integer $a \in \mathbb{Z}$ is an n-th power residue modulo m if and only if the residue class $a + m\mathbb{Z}$ is an n-th power in the residue class ring $\mathbb{Z}/m\mathbb{Z}$. If, moreover, $(a, m) = 1$, then a is an n-th power residue modulo m if and only if $a + m\mathbb{Z}$ is an n-th power in the prime residue class group $(\mathbb{Z}/m\mathbb{Z})^\times$. In this case, if $n = dk$, where $d,\ k \in \mathbb{N}$ and $(d, k) = 1$, then a is an n-th power residue modulo m if and only if a is both a d-th and a k-th power residue modulo m (see Theorem A.5.1.3).

Simple algebraic considerations yield criteria for an integer a to be an n-th power residue for a given modulus m (see the subsequent Theorems 3.1.1, 3.1.2 and 3.1.5). However, given $a \in \mathbb{Z}$, it is a difficult question to characterize those moduli m such that a is a quadratic residue modulo m. Indeed, it is rather simple to say which persons are likable to me, but it is a delicate question to which persons I am likable (this analogy goes back to my teacher Alexander Aigner, see [**1**, p. 128]). The higher reciprocity laws of algebraic number theory connect the n-th power character of a modulo m with the n-th power character of m modulo $|a|$. For $n = 2$, this is done by the quadratic reciprocity law and its refinement by Jacobi. For $n > 2$, this is part of Artin's reciprocity law in class field theory (see [**85**, Ch. VI, §8]).

By the Chinese remainder theorem, we reduce the question of n-th power residues to prime powers, and an elementary argument shows that it suffices to consider prime residues (see Theorem 3.1.1).

Theorem 3.1.1. *Let $n \ge 2$ be an integer.*

1. *Suppose that $m = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$, where $r \in \mathbb{N}$, $p_1, \ldots, p_r$ are distinct primes and $e_1, \ldots, e_r \in \mathbb{N}$. Then an integer a is an n-th power residue modulo m if and only if a is an n-th power residue modulo $p_i^{e_i}$ for all $i \in [1, r]$.*
2. *Let p be a prime, $e \in \mathbb{N}_0$ and $a = p^d b \in \mathbb{Z}$, where $d \in \mathbb{N}_0$, $b \in \mathbb{Z}$ and $p \nmid b$. Then a is an n-th power residue modulo p^e if and only if*
    - *either $d \ge e$,*
    - *or $d < e$, $n \,|\, d$, and b is an n-th power residue modulo p^{e-d}.*

Proof. 1. If $x \in \mathbb{Z}$ and $x^n \equiv a \bmod m$, then obviously $x^n \equiv a \bmod p_i^{e_i}$ for all $i \in [1, r]$. For the converse, assume that, for each $i \in [1, r]$, a is an n-th power residue modulo $p_i^{e_i}$, and let $x_i \in \mathbb{Z}$ be such that $x_i^n \equiv a \bmod p_i^{e_i}$. By the Chinese remainder theorem, there is some $x \in \mathbb{Z}$ such that $x \equiv x_i \bmod p_i^{e_i}$. Then it follows that $x^n \equiv x_i^n \equiv a \bmod p_i^{e_i}$ for all $i \in [1, r]$, hence $x^n \equiv a \bmod m$, and a is an n-th power residue modulo m.

2. If $d \ge e$, then $a \equiv 0^n \bmod p^e$. If $d < e$, $d \,|\, n$ and b is an n-th power residue modulo p^{e-d}, then there exist d, $y \in \mathbb{Z}$ such that $d = nc$ and $y^n \equiv b \bmod p^{e-d}$. With these settings, we obtain $(p^c y)^n \equiv a \bmod p^e$, and thus a is an n-th power residue modulo p^e.

Assume now that $d < e$, and $a = p^d b$ is an n-th power residue modulo p^e, say $x^n \equiv p^d b \bmod p^e$ for some $x \in \mathbb{Z}$. Then $x^n = p^d b + p^e u = p^d(b + p^{e-d} u)$ for some $u \in \mathbb{Z}$, and we set $x = p^c y$, where $c \in \mathbb{N}_0$, $y \in \mathbb{Z}$ and $p \nmid y$. Then it follows that $p^{nc} y^n = p^d(b + p^{e-d} u)$, hence $d = nc$ and $y^n \equiv b \bmod p^{e-d}$. □

Now we do the prime power case, and finally in Theorem 3.1.5 we specialize to quadratic residues modulo prime powers.

Theorem 3.1.2. *Let p be a prime, $e, n \in \mathbb{N}$ and a an integer such that $p \nmid a$.*

1. *If a is an n-th power residue modulo p^e, then*

$$|\{x + p^e\mathbb{Z} \mid x^n \equiv a \bmod p^e\}| = \begin{cases} (n, p^{e-1}(p-1)) & \text{if } p \ne 2\,, \\ 1 & \text{if } p = 2 \nmid n\,, \\ 2^{\min\{e-1, d+1\}} & \text{if } p = 2 \text{ and } \mathsf{v}_2(n) = d \ge 1\,. \end{cases}$$

2. *If $p \nmid n$, then the following assertions are equivalent:*
    - (a) *a is an n-th power residue modulo p^e.*
    - (b) *a is an n-th power residue modulo p.*
    - (c) *$a^{(p-1)/(p-1,n)} \equiv 1 \bmod p$.*

3. *If $d \in \mathbb{N}$, then a is a p^d-th power residue modulo p^e if and only if*

$$\begin{cases} a^{p-1} \equiv 1 \mod p^{\min\{d+1,e\}} & \text{if} \quad p \neq 2\,, \\ a \equiv 1 \mod 2^{\min\{d+2,e\}} & \text{if} \quad p = 2\,. \end{cases}$$

PROOF. Recall that a is an n-th power residue modulo p^e if and only if $a + p^e\mathbb{Z}$ is an n-th power in the residue class group $(\mathbb{Z}/p^e\mathbb{Z})^\times$. Now the proof depends on the following elementary number-theoretical and group-theoretical facts (for details see the Theorems A.6.4 and A.5.2).

A. If $p \neq 2$, then $(\mathbb{Z}/p^e\mathbb{Z})^\times$ is a cyclic group of order $p^{e-1}(p-1)$, and the subgroup $\{x + p^e\mathbb{Z} \mid x \equiv 1 \mod p\} \subset (\mathbb{Z}/p^e\mathbb{Z})^\times$ is of order p^{e-1} and generated by $(1+p) + p^e\mathbb{Z}$.

B. If $e \geq 2$, then $U = \{x + 2^e\mathbb{Z} \mid x \equiv 1 \mod 4\} = \langle 5 + 2^e\mathbb{Z}\rangle$ is a cyclic group of order 2^{e-2}.

C. Let G be a cyclic group with unit element e and $|G| = n$. An element $a \in G$ is an d-th power if and only if $a^{n/(n,d)} = e$, and then $|\{x \in G \mid x^d = a\}| = (n,d)$.

CASE 1: $p \neq 2$. Since $(\mathbb{Z}/p^e\mathbb{Z})^\times$ is cyclic, 1. follows by **C**. By **A** and **B**, a is an n-th power residue modulo p^e if and only if

$$a^B \equiv 1 \mod p^e\,, \quad \text{where} \quad B = \frac{|(\mathbb{Z}/p^e\mathbb{Z})^\times|}{(|(\mathbb{Z}/p^e\mathbb{Z})^\times|, n)} = \frac{p^{e-1}(p-1)}{(p^{e-1}(p-1), n)}\,.$$

If $p \nmid n$, then $(p^{e-1}(p-1), n) = (p-1, n)$. If $x \in \mathbb{Z}$, then $x^{p^{e-1}} \equiv 1 \mod p^e$ if and only if $x \equiv 1 \mod p$. Hence

$$a^B = \big(a^{(p-1)/(p-1,n)}\big)^{p^{e-1}} \equiv 1 \mod p^e \quad \text{if and only if} \quad a^{(p-1)/(p-1,n)} \equiv 1 \mod p\,,$$

and therefore (a), (b) and (c) are equivalent.

If $n = p^d$, then $B = (p-1)p^k$, where $k = e - 1 - \min\{d, e-1\}$, and since $a^{p-1} \equiv 1 \mod p$, there is some $l \in [0, p^{e-1} - 1]$ such that $a^{p-1} \equiv (1+p)^l \mod p^e$. Hence $a^B \equiv (1+p)^{lp^k} \mod p^e$, and we obtain:

$$\begin{aligned} a^B \equiv 1 \mod p^e \iff p^{e-1} \,|\, lp^k \iff p^{\min\{d,e-1\}} \,|\, l \\ \iff (1+p)^l \equiv 1 \mod p^{\min\{d,e-1\}+1} \iff a^{p-1} \equiv 1 \mod p^{\min\{d+1,e\}}\,. \end{aligned}$$

CASE 2: $p = 2$. If $2 \nmid n$, then $(x \mapsto x^n)$ is an automorphism of $(\mathbb{Z}/2^e\mathbb{Z})^\times$, and there is nothing to do. Thus suppose that $n = 2^d u$, where $d = \mathsf{v}_2(n) \geq 1$, $u \in \mathbb{N}$ and $2 \nmid u$. For $e \leq 2$, the assertion is obvious, and thus we assume that $e \geq 3$. By **B** and **C** it follows that

$$|\{x + 2^e\mathbb{Z} \mid x \equiv 1 \mod 4\,,\ x^n \equiv a \mod 2^e\}| = (n, 2^{e-2}) = 2^{\min\{d,e-2\}}\,,$$

and since

$$\begin{aligned} \{x + 2^e\mathbb{Z} \mid x^n \equiv a \mod 2^e\} = \{x + 2^e\mathbb{Z} \mid x \equiv 1 \mod 4\,,\ x^n \equiv a \mod 2^e\} \\ \uplus \{-x + 2^e\mathbb{Z} \mid x \equiv 1 \mod 4\,,\ x^n \equiv a \mod 2^e\}\,, \end{aligned}$$

it follows that

$$|\{x + 2^e\mathbb{Z} \mid x^n \equiv a \mod 2^e\}| = 2 \cdot 2^{\min\{d.e-2\}} = 2^{\min\{d+1,e-1\}}.$$

It remains to prove 3. If $e \geq 2$ and a is an 2^d-th power residue modulo 2^e, then $a \equiv 1 \bmod 4$, hence $a + 2^e\mathbb{Z} \in U$ and $a \equiv 5^l \bmod 2^e$ for some $l \in [0, 2^{e-2} - 1]$. Therefore a is a 2^d-th power residue modulo 2^e if and only if

$$a^B \equiv 1 \mod 2^e\,, \quad \text{where} \quad B = \frac{|U|}{(|U|, n)} = 2^{e-2-\min\{e-2,d\}}.$$

If $k = e - 2 - \min\{e-2, d\}$, then $a^B \equiv 5^{2^k l} \mod 2^e$, and we obtain:

$$\begin{aligned} a^B \equiv 1 \mod 2^e \quad &\Longleftrightarrow \quad 2^{e-2} \,|\, 2^k l \quad \Longleftrightarrow \quad 2^{\min\{d,e-2\}} \,|\, l \\ &\Longleftrightarrow \quad 5^l \equiv 1 \mod 2^{\min\{d,e-2\}+2} \\ &\Longleftrightarrow \quad a \equiv 1 \mod 2^{\min\{d+2,e\}}\,. \end{aligned}$$

□

Example 3.1.3. We use Theorems 3.1.1 and 3.1.2 to determine all $a \in \mathbb{Z}$ which are 36th power residues modulo 864. Since $864 = 2^5 \cdot 3^3$, a is a 36th power residues modulo 864 if and only if it is a 36th power residues modulo 32 and modulo 27.

If $2 \,|\, a$, then a is a 36th power residue modulo 32 if and only if $a \equiv 0 \bmod 32$.

If $2 \nmid a$, then a is a 36th power residue modulo 32 if and only if a is a biquadratic residue modulo 32, and this holds if and only if $a \equiv 1 \bmod 16$.

If $3 \,|\, a$, then a is a 36th power residue modulo 27 if and only if $a \equiv 0 \bmod 27$.

If $3 \nmid a$, then a is a 36th power residue modulo 32 if and only if a is a biquadratic residue and a 9th power residue modulo 27, and this holds if and only if $a \equiv 1 \bmod 3$ and $a^2 \equiv 1 \bmod 27$, which is equivalent to $a \equiv 1 \bmod 27$.

Putting the information together, we obtain: a is a 36th power residues modulo 864 if and only if $a \equiv 352 \bmod 864$ or $a \equiv 0$, 1 or 81 mod 432.

Exercise 3.1.4. Which integers are 9th power residues modulo 18000?

Theorem 3.1.5. *Let a be an integer.*

1. *Let p be an odd prime such that $p \nmid a$ and $e \in \mathbb{N}$. Then the following assertions are equivalent:*
   - (a) *a is a quadratic residue modulo p^e.*
   - (b) *a is a quadratic residue modulo p.*
   - (c) $a^{(p-1)/2} \equiv 1 \bmod p$.

   If a is a quadratic non-residue modulo p, then $a^{(p-1)/2} \equiv -1 \bmod p$.
2. *If $2 \nmid a$ and $e \in \mathbb{N}$, then a is a quadratic residue modulo 2^e if and only if*
   - *either* $e = 1$
   - *or* $e = 2$ *and* $a \equiv 1 \bmod 4$
   - *or* $e \geq 3$ *and* $a \equiv 1 \bmod 8$.
3. *Suppose that $m = 2^e p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$, where $e, r \in \mathbb{N}_0$, $e_1, \ldots, e_r \in \mathbb{N}$, $p_1, \ldots, p_r$ are distinct odd primes, and $(m, a) = 1$. Then a is a quadratic residue modulo m if and only if the following assertions hold:*
   - *For all $i \in [1, r]$, a is a quadratic residue modulo p_i.*

- *If* $e=2$, *then* $a \equiv 1 \bmod 4$.
- *If* $e \ge 3$, *then* $a \equiv 1 \bmod 8$.

If these conditions are fulfilled and $\delta = \min\{2, e-1\}$, *then*

$$|\{x + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})^\times \mid x^2 \equiv a \mod m\}| = 2^{r+\delta}\,.$$

PROOF. 1. and 2. The criteria for quadratic residues follow by Theorem 3.1.2. If p is an odd prime and $a \in \mathbb{Z} \setminus p\mathbb{Z}$, then $a^{(p-1)/2} \equiv \pm 1 \bmod p$ by Theorem A.6.3.3. Consequently, if a is a quadratic non-residue modulo p, then $a^{(p-1)/2} \equiv -1 \bmod p$.

3. Obvious by 1., 2., Theorem 3.1.1 and Theorem 3.1.2.1. □

Later, in Theorem 3.5.11, we shall give another formula for the number of solutions of a quadratic congruence using Kronecker symbols.

3.2. Gauss and Jacobi sums

A reader not familiar with roots of unity, group characters and algebraic integers should consult the Sections A.7, A.8 and A.9. Throughout, let $\overline{\mathbb{Z}}$ be the ring of all algebraic integers, and for $m \in \mathbb{N}$ we the denote by $\zeta_m = \mathsf{e}^{2\pi \mathsf{i}/m}$ the normalized primitive m-th root of unity.

In this section we specialize the general theory of group characters to residue class characters and Dirichlet characters. For these, we investigate Gauss and Jacobi sums, notions which will further be used in the Chapters 4, 7 and 8.

For $m \in \mathbb{N}$, we denote by $\mathsf{X}(m) = \mathrm{Hom}((\mathbb{Z}/m\mathbb{Z})^\times, \mathbb{C}^\times)$ the character group of $(\mathbb{Z}/m\mathbb{Z})^\times$ (equipped with point-wise multiplication) and call its elements *characters modulo* m. The unit element $\mathbf{1}_m \in \mathsf{X}(m)$ (the constant character with value 1) is called the *principal character modulo* m. Note that $|\mathsf{X}(m)| = |(\mathbb{Z}/m\mathbb{Z})^\times| = \varphi(m)$ (Euler's φ function). Hence, if $\chi \in \mathsf{X}(m)$, then $d = \mathrm{ord}(\chi) \,|\, \varphi(m)$, and the values $\chi(t)$ for $t \in (\mathbb{Z}/m\mathbb{Z})^\times$ are d-th roots of unity. A character $\chi \in \mathsf{X}(m)$ is called

- *real* if $\chi^2 = \mathbf{1}_m$ [equivalently, $\chi(t) \in \{\pm 1\}$ for all $t \in (\mathbb{Z}/m\mathbb{Z})^\times$];
- *quadratic* if $\mathrm{ord}(\chi) = 2$ [equivalently, χ is real and $\chi \ne \mathbf{1}_m$].

If $(\mathbb{Z}/m\mathbb{Z})^\times = \langle \omega \rangle$ is cyclic (for example, if m is an odd prime power), then a character $\chi \in \mathsf{X}(m)$ is uniquely determined by its value $\chi(\omega) \in \mathbb{C}^\times$, we have $\mathrm{ord}(\chi) = \mathrm{ord}(\chi(\omega))$, and $|\{\chi \in \mathsf{X}(m) \mid \mathrm{ord}(\chi) = d\}| = \varphi(d)$. In particular, if $m \ge 3$ and $(\mathbb{Z}/m\mathbb{Z})^\times = \langle \omega \rangle$, then there exists a unique quadratic character $\varphi \in \mathbb{X}(m)$, given by $\varphi(\omega^k) = (-1)^k$ for all $k \in \mathbb{Z}$. Quadratic characters will play a central role in this volume and we shall study them in detail from Section 3.3 on.

Let now again $m \in \mathbb{N}$ be arbitrary. For a character $\chi \in \mathsf{X}(m)$, we define

$$\widetilde{\chi}\colon \mathbb{Z} \to \mathbb{C} \quad \text{by} \quad \widetilde{\chi}(a) = \begin{cases} \chi(a + m\mathbb{Z}) & \text{if} \quad (a,m) = 1\,, \\ 0 & \text{if} \quad (a,m) \ne 1\,, \end{cases}$$

and we call the function $\widetilde{\chi}\colon \mathbb{Z} \to \mathbb{C}$ the associated *Dirichlet character* modulo m. As there is no danger of confusion, we will in the sequel always write χ instead of $\widetilde{\chi}$. Therefore, a character $\chi \in \mathsf{X}(m)$ is both a homomorphism $\chi\colon (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$ and a Dirichlet character $\chi\colon \mathbb{Z} \to \mathbb{C}$ modulo m.

Consequently, if $\chi \in \mathsf{X}(m)$, then

- χ is real if and only if $\chi(a) \in \{0, \pm 1\}$ for all $a \in \mathbb{Z}$,
- χ is quadratic if and only if χ is real and $\chi(c) = -1$ for some $c \in \mathbb{Z}$,
- $\chi(ab) = \chi(a)\chi(b)$ for all a, $b \in \mathbb{Z}$, and $\chi(a) = 1$ if $a \equiv 1 \mod m$,
- $\chi(at) = \chi(a)\chi(t)$ for all $a \in \mathbb{Z}$ and $t \in (\mathbb{Z}/m\mathbb{Z})^\times$,

$$\sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(t) = \sum_{j=c}^{c+m-1} \chi(j) = \begin{cases} \varphi(m) & \text{if } \chi = \mathbf{1}_m\,, \\ 0 & \text{if } \chi \neq \mathbf{1}_m \end{cases} \qquad \text{for all } c \in \mathbb{Z}\,,$$

$$\mathbf{1}_m(a) = \begin{cases} 1 & \text{if } (a,m) = 1\,, \\ 0 & \text{if } (a,m) \neq 1 \end{cases} \qquad \text{for all } a \in \mathbb{Z}\,,$$

and $\mathsf{X}(1) = \{\mathbf{1}_1\}$, where $\mathbf{1}_1 = 1 \colon \mathbb{Z} \to \mathbb{C}$ is the constant function with value 1.

Let k, $m \in \mathbb{N}$ be such that $k \,|\, m$, $\psi \in \mathsf{X}(k)$ and $\chi \in \mathsf{X}(m)$. Then χ is said to be *induced* by ψ if $\chi(a) = \psi(a)$ for all $a \in \mathbb{Z}$ satisfying $(a,m) = 1$. A character $\chi \in \mathsf{X}(m)$ is called *primitive* (modulo m) if it is not induced by a character modulo k for some proper positive divisor k of m.

By definition, a character $\chi \in \mathsf{X}(m)$ is primitive if and only if its inverse $\chi^{-1} = \overline{\chi}$ is primitive. If p is a prime, then every character $\chi \in \mathsf{X}(p) \setminus \{\mathbf{1}_p\}$ is primitive. The unit character $\mathbf{1}_m$ is induced by $\mathbf{1}_1$, and therefore $\mathbf{1}_m$ is primitive if and only if $m = 1$.

For a character $\chi \in \mathsf{X}(m)$ and $\alpha \in \mathbb{Z}/m\mathbb{Z}$, we define the *Gauss sum* attached with χ and α by

$$\tau(\chi, \alpha) = \sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(t)\zeta_m^{\alpha t}\,, \quad \text{where} \quad \zeta_m = \mathsf{e}^{2\pi \mathsf{i}/m}\,.$$

For $a \in \mathbb{Z}$, we set $\tau(\chi, a) = \tau(\chi, a + m\mathbb{Z})$, and we define

$$\tau(\chi) = \tau(\chi, 1) = \sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(t)\zeta_m^t = \sum_{j=0}^{m-1} \chi(j)\zeta_m^j\,.$$

Since $|\mathsf{X}(m)| = \varphi(m)$ it follows that $\chi(t) \in \mathbb{Z}[\zeta_{\varphi(m)}]$ and $\tau(\chi, a) \in \mathbb{Z}[\zeta_{m\varphi(m)}] \subset \overline{\mathbb{Z}}$ for all $\chi \in \mathsf{X}(m)$, $t \in (\mathbb{Z}/m\mathbb{Z})^\times$ and $a \in \mathbb{Z}$.

Theorem 3.2.1. *Let m be a positive integer and $\chi \in \mathsf{X}(m)$.*

1. *χ is primitive if and only if for every proper positive divisor k of m there exists some $a \in \mathbb{Z}$ such that $(a,m) = 1$, $a \equiv 1 \mod k$ and $\chi(a) \neq 1$.*
2. *If $a \in \mathbb{Z}$, then*
$$\overline{\tau(\chi, a)} = \chi(-1)\,\tau(\overline{\chi}, a)\,,$$
and if either $(a,m) = 1$ or χ is primitive, then
$$\tau(\chi, a) = \overline{\chi}(a)\,\tau(\chi)\,.$$
3. *If χ is primitive, then*
$$|\tau(\chi)| = \sqrt{m} \quad \textit{and} \quad \tau(\chi)\tau(\overline{\chi}\,) = \chi(-1)m\,.$$

PROOF. 1. If χ is not primitive, then there exists a proper positive divisor k of m such that χ is induced by some character $\psi \in \mathsf{X}(k)$. In this case, if $a \in \mathbb{Z}$, $(a,m)=1$ and $a \equiv 1 \bmod k$, then $\chi(a) = \psi(a) = \psi(1+k\mathbb{Z}) = 1$.

Assume now that there exists some proper positive divisor k of m with the property that $\chi(a) = 1$ for all $a \in \mathbb{Z}$ satisfying $(a,m)=1$ and $a \equiv 1 \bmod k$. There is a surjective homomorphism $\pi\colon (\mathbb{Z}/m\mathbb{Z})^\times \to (\mathbb{Z}/k\mathbb{Z})^\times$ such that $\pi(a+m\mathbb{Z}) = a+k\mathbb{Z}$ for all $a \in \mathbb{Z}$ such that $(a,m)=1$ (see Theorem A.6.1), and

$$\begin{aligned}\operatorname{Ker}(\pi) &= \{a+m\mathbb{Z} \mid a \in \mathbb{Z},\ (a,m)=1,\ a \equiv 1 \bmod k\} \\ &\subset \operatorname{Ker}\bigl(\chi\colon (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}\bigr).\end{aligned}$$

Hence there exists a unique homomorphism $\psi\colon (\mathbb{Z}/k\mathbb{Z})^\times \to \mathbb{C}^\times$ such that $\psi\circ\pi = \chi$. We obtain $\psi \in \mathsf{X}(k)$, $\psi(a) = \chi(a)$ for all $a \in \mathbb{Z}$ such that $(a,m)=1$, and χ is induced by ψ.

2. For $s \in (\mathbb{Z}/m\mathbb{Z})^\times$, we have $\overline{\chi}(-s) = \overline{\chi}(-1)\overline{\chi}(s) = \chi(-1)\overline{\chi}(s)$. Hence

$$\begin{aligned}\overline{\tau(\chi,a)} &= \sum_{t\in(\mathbb{Z}/m\mathbb{Z})^\times} \overline{\chi}(t)\zeta_m^{-at} \underset{[s=-t]}{=} \sum_{s\in(\mathbb{Z}/m\mathbb{Z})^\times} \overline{\chi}(-s)\zeta_m^{as} \\ &= \chi(-1) \sum_{s\in(\mathbb{Z}/m\mathbb{Z})^\times} \overline{\chi}(s)\zeta_m^{as} = \chi(-1)\tau(\overline{\chi},a).\end{aligned}$$

If $(a,m)=1$, then

$$\chi(a)\,\tau(\chi,a) = \sum_{t\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(at)\zeta_m^{at} \underset{[s=at]}{=} \sum_{s\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(s)\zeta_m^{s} = \tau(\chi),$$

and therefore $\tau(\chi,a) = \overline{\chi}(a)\chi(a)\tau(\chi,a) = \overline{\chi}(a)\tau(\chi)$.

Assume now that χ is primitive and $(a,m) = d > 1$. Then $\overline{\chi}(a) = 0$, and we must prove that $\tau(\chi,a) = 0$. Suppose that $a = db$ and $m = dk$, where $b,\, k \in \mathbb{N}$. By 1., there exists some $c \in \mathbb{Z}$ such that $(c,m)=1$, $c \equiv 1 \bmod k$ and $\chi(c) \ne 1$. For all $t \in (\mathbb{Z}/m\mathbb{Z})^\times$, we obtain $\zeta_m^{at} = \zeta_m^{dbt} = \zeta_k^{bt} = \zeta_k^{btc} = \zeta_m^{dbtc} = \zeta_m^{atc}$, hence

$$\begin{aligned}\chi(c)\,\tau(\chi,a) &= \sum_{t\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(ct)\zeta_m^{at} = \sum_{t\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(ct)\zeta_m^{atc} \\ &\underset{[s=ct]}{=} \sum_{s\in(\mathbb{Z}/m\mathbb{Z})^\times} \chi(s)\zeta_m^{as} = \tau(\chi,a), \quad \text{and thus} \quad \tau(\chi,a) = 0.\end{aligned}$$

3. We calculate

$$\begin{aligned}|\tau(\chi)|^2 &= \tau(\chi)\overline{\tau(\chi)} = \tau(\chi)\sum_{\nu=0}^{m-1} \overline{\chi}(\nu)\zeta_m^{-\nu} = \sum_{\nu=0}^{m-1} \tau(\chi,\nu)\zeta_m^{-\nu} = \sum_{\nu=0}^{m-1}\sum_{\mu=0}^{m-1} \chi(\mu)\zeta_m^{\mu\nu-\nu} \\ &= \sum_{\mu=0}^{m-1} \chi(\mu)\sum_{\nu=0}^{m-1} \zeta_m^{(\mu-1)\nu} = m, \quad \text{since} \quad \sum_{\nu=0}^{m-1} \zeta_m^{(\mu-1)\nu} = \begin{cases} 0 & \text{if} \quad \mu \ne 1, \\ m & \text{if} \quad \mu = 1. \end{cases}\end{aligned}$$

Hence $|\tau(\chi)| = \sqrt{m}$, and $m = |\tau(\chi)|^2 = \tau(\chi)\overline{\tau(\chi)} = \chi(-1)\tau(\chi)\tau(\overline{\chi}\,)$, which implies $\tau(\chi)\tau(\overline{\chi}\,) = \chi(-1)m$. □

Exercise 3.2.2. Let p be a prime and $\chi \in \mathsf{X}(p)$. Calculate

$$\sum_{\alpha \in \mathbb{F}_p} \tau(\chi, \alpha)\,.$$

Exercise 3.2.3. Suppose that $m,\ k \in \mathbb{N},\ \ n = mk,\ \ a \in \mathbb{Z}$ and $\chi \in \mathsf{X}(m)$. Prove that

$$\sum_{j=0}^{n-1} \chi(j)\zeta_n^{aj} = \begin{cases} 0 & \text{if} \quad k \nmid a\,, \\ k\,\overline{\chi}(k^{-1}a)\tau(\chi) & \text{if} \quad k \mid a\,. \end{cases}$$

Next we introduce Jacobi sums and investigate their connection with Gauss sums. For an odd prime p and characters $\chi_1,\ \chi_2 \in \mathsf{X}(p)$, we define the *Jacobi sum* $\mathsf{J}(\chi_1, \chi_2) \in \overline{\mathbb{Z}}$ by

$$\mathsf{J}(\chi_1, \chi_2) = \sum_{a \in \mathbb{F}_p^\times \setminus \{1\}} \chi_1(a)\,\chi_2(1-a)\,.$$

If $d \in \mathbb{N}$ is such that $\chi_1^d = \chi_2^d = \mathbf{1}_p$, then $\mathsf{J}(\chi_1, \chi_2) \in \mathbb{Z}[\zeta_d]$.

Theorem 3.2.4. *Let p be an odd prime and $\chi,\ \chi_1,\ \chi_2 \in \mathsf{X}(p) \setminus \{\mathbf{1}_p\}$.*

1. $\mathsf{J}(\mathbf{1}_p, \mathbf{1}_p) = p-2,\ \ \tau(\mathbf{1}_p) = \mathsf{J}(\chi, \mathbf{1}_p) = -1$ *and* $\mathsf{J}(\chi, \chi^{-1}) = -\chi(-1)$.
2. *If* $\chi_1\chi_2 \neq \mathbf{1}_p$, *then* $\tau(\chi_1)\tau(\chi_2) = \tau(\chi_1\chi_2)\,\mathsf{J}(\chi_1, \chi_2)$, *and* $|\mathsf{J}(\chi_1, \chi_2)| = \sqrt{p}$.
3. *If* $\operatorname{ord}(\chi) = n$, *then*

$$\tau(\chi)^n = p\,\chi(-1) \prod_{k=1}^{n-2} \mathsf{J}(\chi, \chi^k)\,.$$

PROOF. 1. By definition, $\mathsf{J}(\mathbf{1}_p, \mathbf{1}_p) = p-2$,

$$\tau(\mathbf{1}_p) = \sum_{t \in \mathbb{F}_p^\times} \zeta_p^t = \sum_{t \in \mathbb{F}_p} \zeta_p^t - 1 = -1\,, \quad \mathsf{J}(\chi, \mathbf{1}_p) = \sum_{t \in \mathbb{F}_p^\times \setminus \{1\}} \chi(t) = \sum_{t \in \mathbb{F}_p^\times} \chi(t) - 1 = -1\,,$$

and

$$\mathsf{J}(\chi, \chi^{-1}) = \sum_{a \in \mathbb{F}_p^\times \setminus \{1\}} \chi(a)\chi^{-1}(1-a) = \sum_{a \in \mathbb{F}_p^\times \setminus \{1\}} \chi\Big(\frac{a}{1-a}\Big)\,.$$

The map $g \colon \mathbb{F}_p^\times \setminus \{1\} \to \mathbb{F}_p^\times \setminus \{-1\}$, defined by

$$g(a) = \frac{a}{1-a}\,, \quad \text{is bijective} \ \Big[\text{its inverse is given by } \ g^{-1}(b) = \frac{b}{1+b}\,\Big]\,,$$

and therefore

$$\mathsf{J}(\chi, \chi^{-1}) = \sum_{b \in \mathbb{F}_p^\times \setminus \{-1\}} \chi(b) \ = \sum_{b \in \mathbb{F}_p^\times} \chi(b) \ - \ \chi(-1) = -\chi(-1)\,.$$

2. If $\chi_1\chi_2 \neq \mathbf{1}$, then

$$\begin{aligned}
&\tau(\chi_1)\tau(\chi_2)\\
&\quad= \sum_{t\in\mathbb{F}_p^\times}\sum_{s\in\mathbb{F}_p^\times}\chi_1(s)\chi_2(t)\zeta_p^{s+t} = \sum_{t\in\mathbb{F}_p}\sum_{s\in\mathbb{F}_p}\chi_1(s)\chi_2(t)\zeta_p^{s+t} \underset{[u=s+t]}{=}\\
&\quad= \sum_{u\in\mathbb{F}_p}\sum_{s\in\mathbb{F}_p}\chi_1(s)\chi_2(u-s)\zeta_p^u \;=\; \sum_{u\in\mathbb{F}_p}\sum_{s\in\mathbb{F}_p^\times}\chi_1(s)\chi_2(u-s)\zeta_p^u\\
&\quad= \chi_2(-1)\sum_{s\in\mathbb{F}_p^\times}(\chi_1\chi_2)(s) + \sum_{u\in\mathbb{F}_p^\times}\sum_{s\in\mathbb{F}_p^\times}\chi_1(u)\chi_2(u)\chi_1\Big(\frac{s}{u}\Big)\chi_2\Big(1-\frac{s}{u}\Big)\zeta_p^u \underset{[\frac{s}{u}=v]}{=}\\
&\quad= \sum_{u\in\mathbb{F}_p^\times}(\chi_1\chi_2)(u)\zeta_p^u\sum_{v\in\mathbb{F}_p^\times\setminus\{1\}}\chi_1(v)\chi_2(1-v) = \tau(\chi_1\chi_2)\,\mathsf{J}(\chi_1,\chi_2)\,.
\end{aligned}$$

Since $|\tau(\chi_1)| = |\tau(\chi_2)| = |\tau(\chi_1\chi_2)| = \sqrt{p}$, it follows that $|\mathsf{J}(\chi_1,\chi_2)| = \sqrt{p}$, too.

3. We prove first by induction on l that

$$\tau(\chi)^l = \tau(\chi^l)\prod_{k=1}^{l-1}\mathsf{J}(\chi,\chi^k) \quad \text{for all} \quad l \in [1, n-1]\,.$$

For $l = 1$, there is nothing to do.

$l \in [1, n-2]$, $l \to l+1$: Since $\chi^{l+1} \neq \mathbf{1}$, we obtain, using 2. and the induction hypothesis,

$$\tau(\chi)^{l+1} = \tau(\chi)\tau(\chi)^l = \tau(\chi)\tau(\chi^l)\prod_{k=1}^{l-1}\mathsf{J}(\chi,\chi^k) = \tau(\chi^{l+1})\prod_{k=1}^{l}\mathsf{J}(\chi,\chi^k)\,.$$

Now $\chi^{n-1} = \overline{\chi}$, Theorem 3.2.1 implies that $\tau(\chi)\tau(\overline{\chi}) = \chi(-1)p$, and therefore

$$\tau(\chi)^n = \tau(\chi)\tau(\chi)^{n-1} = \tau(\chi)\tau(\chi^{n-1})\prod_{k=1}^{n-2}\mathsf{J}(\chi,\chi^k) = p\,\chi(-1)\prod_{k=1}^{n-2}\mathsf{J}(\chi,\chi^k)\,. \qquad \square$$

As an unexpected application of Jacobi sums we give an elegant proof of Fermat's theorem on sums of two squares. With completely different methods, we have this already done in Theorem 2.1.7, and we shall examine the subject again in Section 3.4 and later on in Chapter 6.

Theorem 3.2.5 (Fermat's theorem on sums of two squares)**.** *A prime p is the sum of two integral squares if and only if either $p = 2$ or $p \equiv 1 \bmod 4$.*

PROOF. Clearly, $2 = 1^2 + 1^2$. Thus let p be an odd prime. If $p = a^2 + b^2$ for some $a,\, b \in \mathbb{Z}$, then $b \equiv a + 1 \bmod 2$, and $p \equiv a^2 + (a+1)^2 \equiv 1 \bmod 4$.

To prove the converse, assume that $p \equiv 1 \bmod 4$. Then $\mathbb{F}_p^\times$ is a cyclic group of order $|\mathbb{F}_p^\times| = p - 1 \equiv 0 \bmod 4$, and therefore there is some character $\chi \in \mathsf{X}(p)$ such that $\mathrm{ord}(\chi) = 4$ (explicitly, if $\mathbb{F}_p^\times = \langle\omega\rangle$, then we may define χ by $\chi(\omega^k) = \mathsf{i}^k$ for all $k \in \mathbb{Z}$). Since $\mathsf{J}(\chi,\chi) \in \mathbb{Z}[\mathsf{i}]$, there exist $a,\, b \in \mathbb{Z}$ such that $\mathsf{J}(\chi,\chi) = a + b\mathsf{i}$, and since $\chi^2 \neq \mathbf{1}_p$, Theorem 3.2.4.2 implies $|\mathsf{J}(\chi,\chi)|^2 = a^2 + b^2 = p$. $\square$

3.3. The quadratic reciprocity law

Let p be an odd prime. For $a \in \mathbb{Z} \setminus p\mathbb{Z}$, we define the *Legendre symbol* of a modulo p by

$$\Big(\frac{a}{p}\Big) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p\,, \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p\,. \end{cases}$$

By definition, the Legendre symbol of a modulo p only depends on the residue class $\alpha = a + p\mathbb{Z} \in \mathbb{F}_p^\times$, and we set

$$\Big(\frac{\alpha}{p}\Big) = \Big(\frac{a}{p}\Big) = \begin{cases} 1 & \text{if } \alpha \in \mathbb{F}_p^{\times 2}\,, \\ -1 & \text{if } \alpha \in \mathbb{F}_p^\times \setminus \mathbb{F}_p^{\times 2}\,. \end{cases}$$

Recall that $\mathbb{F}_p^\times = (\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group of order $p-1$, and an integer w is called a *primitive root* modulo p if $(\mathbb{Z}/p\mathbb{Z})^\times = \langle w + p\mathbb{Z}\rangle$.

If $\mathbb{F}_p^\times = \langle \omega \rangle$, then

$$\Big(\frac{\omega^k}{p}\Big) = (-1)^k \text{ for all } k \in \mathbb{Z}\,, \quad \text{and therefore} \quad \varphi_p = \Big(\frac{\cdot}{p}\Big) \colon \mathbb{F}_p^\times \to \{\pm 1\}$$

is the unique quadratic character modulo p. In accordance with Section 3.2, we view the quadratic character φ_p as a Dirichlet character modulo p, and then we obtain

$$\varphi_p(a) = \varphi_p(\alpha) = \Big(\frac{a}{p}\Big) = \Big(\frac{\alpha}{p}\Big) = 0 \quad \text{if} \quad a \in p\mathbb{Z} \;\text{ and }\; \alpha = a + p\mathbb{Z} = 0 \in \mathbb{F}_p\,.$$

By definition, it follows that

$$\Big(\frac{ab}{p}\Big) = \Big(\frac{a}{p}\Big)\Big(\frac{b}{p}\Big) \quad \text{and} \quad \Big(\frac{ab^2}{p}\Big) = 1 \quad \text{for all} \quad a,\, b \in \mathbb{Z}\,.$$

Theorem 3.3.1 (Euler's criterion)**.** *Let p be an odd prime. If $a \in \mathbb{Z}$, then*

$$\Big(\frac{a}{p}\Big) \equiv a^{(p-1)/2} \mod p\,.$$

In particular,

$$\Big(\frac{-1}{p}\Big) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \mod 4\,, \\ -1 & \text{if } p \equiv 3 \mod 4\,. \end{cases}$$

Proof. If $a \in p\mathbb{Z}$, the assertion is obvious. Thus assume that $a \in \mathbb{Z} \setminus p\mathbb{Z}$. By Theorem 3.1.5.1, we obtain

$$\Big(\frac{a}{p}\Big) = \pm 1 \text{ if and only if } a^{(p-1)/2} \equiv \pm 1 \mod p\,, \qquad \text{hence} \qquad \Big(\frac{a}{p}\Big) \equiv a^{(p-1)/2} \mod p\,.$$

In particular,

$$\Big(\frac{-1}{p}\Big) \equiv (-1)^{(p-1)/2} \mod p, \quad \text{and consequently } \Big(\frac{-1}{p}\Big) = (-1)^{(p-1)/2}. \qquad \square$$

Exercise 3.3.2. Let p and q be primes such that $q = 2p+1$ and $a \in \mathbb{Z} \setminus q\mathbb{Z}$. Prove that

$$a \text{ is a primitive root modulo } q \text{ if and only if } \Big(\frac{a}{q}\Big) = -1 \text{ and } a \not\equiv -1 \mod q\,.$$

Exercise 3.3.3. Let p be an odd prime, $N = (p-1)/2$, $a \in \mathbb{Z} \setminus p\mathbb{Z}$ and

$$n = |\{j \in [1,N] \mid aj + k \equiv 0 \bmod p \text{ for some } k \in [1,N]\,\}|\,.$$

Prove Gauss' lemma (compare [**27**, Sec. 3.5]):

$$\Big(\frac{a}{p}\Big) = (-1)^n\,, \quad \text{and if } a \text{ is positive and odd, then} \quad n \equiv \sum_{j=1}^{(p-1)/2} \Big\lfloor \frac{ja}{p} \Big\rfloor \mod 2\,.$$

Exercise 3.3.4. Let p be an odd prime. For ε_1, $\varepsilon_2 \in \{\pm 1\}$, we set

$$N_p(\varepsilon_1, \varepsilon_2) = \Big|\Big\{n \in [1, p-2] \;\Big|\; \Big(\frac{n}{p}\Big) = \varepsilon_1,\; \Big(\frac{n+1}{p}\Big) = \varepsilon_2\Big\}\Big|\,.$$

Verify the values of the following table:

ε_1	ε_2	$N_p(\varepsilon_1,\varepsilon_2)$ for $p = 4n+1$	$N_p(\varepsilon_1,\varepsilon_2)$ for $p = 4n+3$
1	1	$n-1$	n
1	-1	n	$n+1$
-1	1	n	n
-1	-1	n	n

Hint: Show that

$$4N_p(\varepsilon_1,\varepsilon_2) = \sum_{n=1}^{p-2} \Big[1 + \varepsilon_1\Big(\frac{n}{p}\Big)\Big]\Big[1 + \varepsilon_2\Big(\frac{n+1}{p}\Big)\Big]$$

and

$$\sum_{n=1}^{p-2}\Big(\frac{n(n+1)}{p}\Big) = \sum_{n=1}^{p-2}\Big(\frac{n'^2}{p}\Big)\Big(\frac{n(n+1)}{p}\Big) = -1 \quad (\text{where} \quad nn' \equiv 1 \bmod p)\,.$$

(Compare [**42**, §10.5].)

Theorem 3.3.5.

1. *Let p be an odd prime, $m \in \mathbb{Z} \setminus p\mathbb{Z}$ and $\varphi \in \mathsf{X}(m)$ a primitive real character modulo m. Then*

$$\varphi(p) = \Big(\frac{\varphi(-1)m}{p}\Big)\,.$$

2. *Let p be an odd prime. Then*

$$\Big(\frac{2}{p}\Big) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \textit{if} \quad p \equiv \pm 1 \mod 8\,, \\ -1 & \textit{if} \quad p \equiv \pm 3 \mod 8\,, \end{cases}$$

and

$$\Big(\frac{-2}{p}\Big) = \begin{cases} 1 & \textit{if} \quad p \equiv 1 \textit{ or } 3 \mod 8\,, \\ -1 & \textit{if} \quad p \equiv 5 \textit{ or } 7 \mod 8\,. \end{cases}$$

3. (Quadratic reciprocity law for the Legendre symbol) *Let p and q be distinct odd primes. Then*

$$\Big(\frac{p}{q}\Big)\Big(\frac{q}{p}\Big) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} -1 & \textit{if} \quad p \equiv q \equiv 3 \mod 4\,, \\ 1 & \textit{otherwise}, \end{cases}$$

and

$$\Big(\frac{p}{q}\Big) = \Big(\frac{q^*}{p}\Big)\,, \quad \textit{where} \quad q^* = (-1)^{(q-1)/2}q\,.$$

Proof. 1. We calculate the Gauss sum $\tau(\varphi) \in \overline{\mathbb{Z}}$ modulo p (we refer to the Appendices A.8 and A.9 for the elementary arithmetic of algebraic integers and congruences between them). Since $\varphi^p = \varphi = \overline{\varphi}$, we obtain

$$\tau(\varphi)^p = \Big(\sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} \varphi(t)\zeta_m^t\Big)^p \equiv \sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} \varphi(t)\zeta_m^{pt} = \tau(\varphi, p) = \varphi(p)\tau(\varphi) \mod p\,,$$

and therefore

$$\tau(\varphi)^{p+1} = \big[\tau(\varphi)^2\big]^{(p-1)/2}\tau(\varphi)^2 \equiv \varphi(p)\tau(\varphi)^2 \mod p\,.$$

Since $\tau(\varphi)^2 = \varphi(-1)m$ and $(\varphi(-1)m, p) = 1$, we may cancel $\tau(\varphi)^2$ from this congruence and obtain, using Theorem 3.3.1,

$$\Big(\frac{\varphi(-1)m}{p}\Big) \equiv \big[\tau(\varphi)^2\big]^{(p-1)/2} \equiv \varphi(p) \mod p\,, \quad \text{and thus} \quad \Big(\frac{\varphi(-1)m}{p}\Big) = \varphi(p)\,.$$

2. Let $\chi\colon (\mathbb{Z}/8\mathbb{Z})^\times \to \{\pm 1\}$ be defined for $a \in \mathbb{Z} \setminus 2\mathbb{Z}$ by

$$\chi(a + 8\mathbb{Z}) = (-1)^{(a^2-1)/8} = (-1)^{(a-1)(a+1)/8} = \begin{cases} 1 & \text{if} \quad p \equiv \pm 1 \mod 8\,, \\ -1 & \text{if} \quad p \equiv \pm 3 \mod 8\,. \end{cases}$$

Then $\chi \in \mathsf{X}(8)$ is a primitive quadratic character modulo 8, $\chi(-1) = 1$, and 1. implies

$$\Big(\frac{2}{p}\Big) = \Big(\frac{\chi(-1)8}{p}\Big) = \chi(p) = (-1)^{(p^2-1)/8}\,.$$

Hence it follows also that

$$\Big(\frac{-2}{p}\Big) = \Big(\frac{-1}{p}\Big)\Big(\frac{2}{p}\Big) = (-1)^{(p-1)/2}\Big(\frac{2}{p}\Big) = \begin{cases} 1 & \text{if} \quad p \equiv 1 \text{ or } 3 \mod 8, \\ -1 & \text{if} \quad p \equiv 5 \text{ or } 7 \mod 8. \end{cases}$$

3. The quadratic character $\varphi_q \in \mathsf{X}(q)$ is primitive. Hence 1. implies that

$$\Big(\frac{p}{q}\Big) = \varphi_q(p) = \Big(\frac{\varphi_q(-1)q}{p}\Big) = \Big(\frac{(-1)^{(q-1)/2}q}{p}\Big) = \Big(\frac{q^*}{p}\Big) = \Big(\frac{-1}{p}\Big)^{(q-1)/2}\Big(\frac{q}{p}\Big),$$

and therefore we obtain

$$\Big(\frac{p}{q}\Big)\Big(\frac{q}{p}\Big) = \Big(\frac{-1}{p}\Big)^{(q-1)/2} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} -1 & \text{if} \quad p \equiv q \equiv 3 \mod 4\,, \\ 1 & \text{otherwise.} \end{cases}$$

The second formula is now obvious. □

Examples 3.3.6. Let p be an odd prime.

1. If $p \neq 3$, then

$$\Big(\frac{-3}{p}\Big) = \Big(\frac{p}{3}\Big) = 1 \quad \text{if and only if} \quad p \equiv 1 \mod 3\,,$$

and

$$\Big(\frac{3}{p}\Big) = \Big(\frac{-1}{p}\Big)\Big(\frac{p}{3}\Big) = 1 \quad \text{if and only if} \quad \Big(\frac{-1}{p}\Big) = \Big(\frac{3}{p}\Big)\,.$$

Hence -3 is a quadratic residue modulo p if and only if $p \equiv 1 \mod 3$, and 3 is a quadratic residue modulo p if and only if $p \equiv \pm 1 \mod 12$.

2. If $p \nmid 6$, then

$$\Big(\frac{6}{p}\Big) = \Big(\frac{3}{p}\Big)\Big(\frac{2}{p}\Big) = 1 \quad \text{if and only if} \quad \Big(\frac{3}{p}\Big) = \Big(\frac{2}{p}\Big)\,.$$

and

$$\Big(\frac{-6}{p}\Big) = \Big(\frac{-3}{p}\Big)\Big(\frac{2}{p}\Big) = 1 \quad \text{if and only if} \quad \Big(\frac{-3}{p}\Big) = \Big(\frac{2}{p}\Big)\,.$$

By 1. and Theorem 3.3.5.2 it follows that 6 is a quadratic residue modulo p if and only if $p \equiv \pm 1$ or $\pm 5 \mod 24$, and -6 is a quadratic residue modulo p if and only if $p \equiv 1,\ 5,\ 7$ or $11 \mod 24$.

Exercise 3.3.7. For each $m \in \{5,\ 7,\ 10,\ 11,\ 13\}$ determine all odd primes $p \nmid m$ such that m is a quadratic residue modulo p (observe that this only depends on the residue class of p modulo $4m$; why?).

Exercise 3.3.8. Determine all odd primes p such that -4 is a biquadratic residue modulo p. Hint: Theorem 3.1.2.

In the sequel we extend the Legendre symbol to symbols with a larger domain of definition. First, we introduce the Jacobi symbol which is defined for arbitrary odd positive denominators. With this extension, the close connection with quadratic residues gets lost, but we attain an efficient tool to calculate Legendre symbols. As a further extension, we introduce Kronecker symbols. These are defined for arbitrary denominators and play an important role in the theory of quadratic forms.

Let $n = p_1 \cdot \ldots \cdot p_r$ be an odd positive integer, where $r \in \mathbb{N}_0$ and $p_1, \ldots, p_r$ are (not necessarily distinct) odd primes. For any $N \in \mathbb{Z}$, we define the *Jacobi symbol* using Legendre symbols by

$$\Big(\frac{N}{n}\Big) = \prod_{i=1}^{r} \Big(\frac{N}{p_i}\Big) \in \{0, \pm 1\}\,.$$

In particular, if n is an odd prime, then the Jacobi symbol coincides with the Legendre symbol. Note that

$$\Big(\frac{N}{n}\Big) = 0 \quad \text{if} \quad (N, n) \neq 1\,.$$

Theorem 3.3.9. *Let $n, n' \in \mathbb{N}$ be odd and $N, N' \in \mathbb{Z}$.*

1. *If $N \equiv N' \bmod p$ for all primes p satisfying $\mathsf{v}_p(n) \equiv 1 \bmod 2$, then*

$$\Big(\frac{N}{n}\Big) = \Big(\frac{N'}{n}\Big)\,.$$

2. *The Jacobi symbol is multiplicative in both variables, that is,*

$$\Big(\frac{N}{nn'}\Big) = \Big(\frac{N}{n}\Big)\Big(\frac{N}{n'}\Big) \quad \textit{and} \quad \Big(\frac{NN'}{n}\Big) = \Big(\frac{N}{n}\Big)\Big(\frac{N'}{n}\Big)\,.$$

3. *Suppose that $\varepsilon = (-1)^{(n-1)/2}$. Then*

$$\Big(\frac{-1}{n}\Big) = \varepsilon = \begin{cases} 1 & \textit{if} \quad n \equiv 1 \bmod 4\,, \\ -1 & \textit{if} \quad n \equiv 3 \bmod 4\,, \end{cases}$$

$$\Big(\frac{2}{n}\Big) = (-1)^{(n^2-1)/8} = (-1)^{(n-\varepsilon)/4} = \begin{cases} 1 & \textit{if } n \equiv \pm 1 \bmod 8, \\ -1 & \textit{if } n \equiv \pm 3 \bmod 8, \end{cases}$$

and

$$\Big(\frac{-2}{n}\Big) = \begin{cases} 1 & \textit{if} \quad n \equiv 1 \textit{ or } 3 \bmod 8\,, \\ -1 & \textit{if} \quad n \equiv 5 \textit{ or } 7 \bmod 8\,. \end{cases}$$

4. (Quadratic reciprocity law for the Jacobi symbol) *If $2 \nmid N$, then*

$$\Big(\frac{N}{n}\Big)\Big(\frac{n}{|N|}\Big) = (-1)^{\frac{n-1}{2}\frac{N-1}{2}}$$

and

$$\Big(\frac{n}{|N|}\Big) = \Big(\frac{N^*}{n}\Big), \quad \textit{where} \quad N^* = (-1)^{(N-1)/2}N\,.$$

5. *If $n \equiv n' \bmod 4|N|$, then*

$$\Big(\frac{N}{n}\Big) = \Big(\frac{N}{n'}\Big)\,.$$

PROOF. 1. If $N \equiv N'$ mod p for all primes p such that $\mathsf{v}_p(n) \equiv 1$ mod 2, then

$$\Big(\frac{N}{n}\Big) = \prod_{\substack{p\in\mathbb{P}\\ \mathsf{v}_p(n)\equiv 1 \bmod 2}} \Big(\frac{N}{p}\Big) = \prod_{\substack{p\in\mathbb{P}\\ \mathsf{v}_p(n)\equiv 1 \bmod 2}} \Big(\frac{N'}{p}\Big) = \Big(\frac{N'}{n}\Big).$$

2. The first assertion follows by the very definition. If $n = p_1 \cdot \ldots \cdot p_r$ for some $r \in \mathbb{N}_0$ and odd primes $p_1, \ldots, p_r$, then we obtain

$$\Big(\frac{NN'}{n}\Big) = \prod_{i=1}^r \Big(\frac{NN'}{p_i}\Big) = \prod_{i=1}^r \Big(\frac{N}{p_i}\Big) \prod_{i=1}^r \Big(\frac{N'}{p_i}\Big) = \Big(\frac{N}{n}\Big)\Big(\frac{N'}{n}\Big).$$

3. Suppose that $n = p_1 \cdot \ldots \cdot p_r$, where $r \in \mathbb{N}_0$ and $p_1, \ldots, p_r$ are odd primes. By 2. and quadratic reciprocity it follows that

$$\Big(\frac{-1}{n}\Big) = \prod_{i=1}^r (-1)^{(p_i-1)/2}, \quad \Big(\frac{2}{n}\Big) = \prod_{i=1}^r (-1)^{(p_i^2-1)/8} \quad \text{and}$$
$$\Big(\frac{-2}{n}\Big) = \Big(\frac{-1}{n}\Big)\Big(\frac{2}{n}\Big).$$

Now the assertion holds since (by Lemma A.3.4)

$$\sum_{i=1}^r \frac{p_i-1}{2} \equiv \frac{n-1}{2} \mod 2, \quad \sum_{i=1}^r \frac{p_i^2-1}{8} \equiv \frac{n^2-1}{8} \mod 2,$$

and if $n = 4m + \varepsilon$, where $m \in \mathbb{N}_0$, then

$$\frac{n^2-1}{8} = 2m^2 + m\varepsilon \equiv m = \frac{n-\varepsilon}{4} \mod 2.$$

4. We may assume that $(N, n) = 1$.

CASE 1: $N > 0$. Set $N = P_1 \cdot \ldots \cdot P_s$ and $n = p_1 \cdot \ldots \cdot p_r$, where $r, s \in \mathbb{N}_0$ and $P_1, \ldots, P_s, p_1, \ldots, p_r$ are odd primes. Then the quadratic reciprocity law for the Legendre symbol implies

$$\Big(\frac{N}{n}\Big)\Big(\frac{n}{N}\Big) = \prod_{i=1}^r \prod_{j=1}^s \Big(\frac{P_j}{p_i}\Big)\Big(\frac{p_i}{P_j}\Big) = (-1)^A,$$
$$\text{where} \quad A = \sum_{i=1}^r \sum_{j=1}^s \frac{P_j-1}{2}\,\frac{p_i-1}{2},$$

and, as above,

$$A = \Big(\sum_{i=1}^r \frac{p_i-1}{2}\Big)\Big(\sum_{j=1}^s \frac{P_j-1}{2}\Big) \equiv \frac{n-1}{2}\,\frac{N-1}{2} \mod 2.$$

CASE 2: $N < 0$. By 3. and CASE 1 we obtain

$$\Big(\frac{N}{n}\Big)\Big(\frac{n}{|N|}\Big) = \Big(\frac{-1}{n}\Big)\Big(\frac{|N|}{n}\Big)\Big(\frac{n}{|N|}\Big) = (-1)^{\frac{n-1}{2} + \frac{n-1}{2}\frac{|N|-1}{2}} = (-1)^{\frac{n-1}{2}\frac{N-1}{2}}.$$

Finally, in both cases, we get

$$\Big(\frac{n}{|N|}\Big) = (-1)^{\frac{n-1}{2}\,\frac{N-1}{2}}\Big(\frac{N}{n}\Big) = \Big(\frac{-1}{n}\Big)^{(N-1)/2}\Big(\frac{N}{n}\Big) = \Big(\frac{N^*}{n}\Big).$$

5. We may assume that $(n, N) = (n', N) = 1$, and $N = (-1)^\alpha 2^\beta p_1 \cdot \ldots \cdot p_r$, where α, β, $r \in \mathbb{N}_0$ and $p_1, \ldots p_r$ are odd primes. If $n \equiv n' \mod 4|N|$, then it follows that $n \equiv n' \mod p_i$ for all $i \in [1, r]$, $n \equiv n' \mod 4$, and even $n \equiv n' \mod 8$ if $\beta > 0$. Hence we obtain

$$\begin{aligned}\Big(\frac{p_i}{n}\Big) &= \Big(\frac{n}{p_i}\Big)(-1)^{\frac{p_i-1}{2}\,\frac{n-1}{2}} = \Big(\frac{n'}{p_i}\Big)(-1)^{\frac{p_i-1}{2}\,\frac{n'-1}{2}} \\ &= \Big(\frac{p_i}{n'}\Big) \quad \text{for all} \quad i \in [1, r],\end{aligned}$$

$$\Big(\frac{(-1)^\alpha 2^\beta}{n}\Big) = \Big(\frac{(-1)^\alpha 2^\beta}{n'}\Big),$$

and

$$\Big(\frac{N}{n}\Big) = \Big(\frac{(-1)^\alpha 2^\beta}{n}\Big)\prod_{i=1}^{r}\Big(\frac{p_i}{n}\Big) = \Big(\frac{(-1)^\alpha 2^\beta}{n'}\Big)\prod_{i=1}^{r}\Big(\frac{p_i}{n'}\Big) = \Big(\frac{N}{n'}\Big). \qquad \square$$

We demonstrate the use of Jacobi symbols and the quadratic reciprocity law for the calculation of Legendre symbols by a numerical example. We verify that -874 is a quadratic residue modulo 5399 (which is prime!) by means of the following calculations.

$$\begin{aligned}\Big(\frac{-874}{5399}\Big) &= \Big(\frac{-1}{5399}\Big)\Big(\frac{2}{5399}\Big)\Big(\frac{19}{5399}\Big)\Big(\frac{23}{5399}\Big) = (-1)\cdot 1 \cdot \Big[-\Big(\frac{5399}{19}\Big)\Big]\cdot\Big[-\Big(\frac{5399}{23}\Big)\Big] \\ &= (-1)\cdot 1\cdot(-1)\cdot\Big[-\Big(\frac{17}{23}\Big)\Big] = -\Big(\frac{17}{23}\Big) = -\Big(\frac{23}{17}\Big) = -\Big(\frac{6}{17}\Big) \\ &= -\Big(\frac{2}{17}\Big)\Big(\frac{3}{17}\Big) = -\Big(\frac{3}{17}\Big) = -\Big(\frac{17}{3}\Big) = -\Big(\frac{2}{3}\Big) = 1\,.\end{aligned}$$

Exercise 3.3.10. Suppose that $m, n \in \mathbb{N}$, $(m, 2n) = 1$, and n is a quadratic residue modulo m. Prove that $\big(\frac{n}{m}\big) = 1$. Show by an example that the converse need not be true.

Occasionally, we shall use the Jacobi symbol for fractional arguments as follows (compare Theorem and Definition A.8.5). Suppose that $n \in \mathbb{N}$ and $z = c^{-1}a \in \mathbb{Z}_{[n]}^\times$, where a, $c \in \mathbb{Z}$ and $(a, n) = (c, n) = 1$. Then we define

$$\Big(\frac{z}{n}\Big) = \Big(\frac{c}{n}\Big)\Big(\frac{a}{n}\Big).$$

Obviously, this definition depends only on z (and not on a and c); the map

$$\Big(\frac{\cdot}{n}\Big) \colon \mathbb{Z}_{[n]}^\times \;\to\; \{\pm 1\}$$

is a homomorphism and induces a homomorphism

$$(\mathbb{Z}_{[n]}/n\mathbb{Z}_{[n]})^\times = (\mathbb{Z}/n\mathbb{Z})^\times \;\to\; \{\pm 1\}\,.$$

3.4. Sums of two squares

In the Theorems 2.1.7.3 and 3.2.5 we proved that every prime $p \equiv 1 \bmod 4$ is the sum of two integral squares. We continue with a more comprehensive investigation of sums of two squares. We will return to the subject again in Chapter 6. There we shall reprove Theorem 3.4.1 and provide also quantitative results using the theory of binary quadratic forms.

Theorem 3.4.1. *Let m be a positive integer.*

1. *m is the sum of two coprime integral squares if and only if $4 \nmid m$, and $p \nmid m$ for all primes $p \equiv 3 \bmod 4$.*
2. *m is the sum of two integral squares if and only if $2 \,|\, \mathsf{v}_p(m)$ for all primes $p \equiv 3 \bmod 4$.*
3. *$m = 4a^2 + b^2$ for some $a,\, b \in \mathbb{N}$ such that $(a,b) = 1$ if and only if $m > 1$ and*
    - *either $m \equiv 1 \bmod 4$ and m is the sum of two coprime integral squares,*
    - *or $m = 4m_0$, where $m_0 \in \mathbb{N}$, $m_0 \equiv 2 \bmod 4$, and m_0 is the sum of two coprime integral squares.*

PROOF. 1. Suppose first that $m = a^2 + b^2$, where $a,\, b \in \mathbb{Z}$ and $(a,b) = 1$. Then it follows that $m \equiv 1$ or $2 \bmod 4$ and thus $4 \nmid m$. If p is an odd prime dividing m, then $p \nmid ab$, and $-a^2 \equiv b^2 \bmod p$. Hence $-a^2$ is a quadratic residue modulo p,

$$1 = \Big(\frac{-a^2}{p}\Big) = \Big(\frac{-1}{p}\Big), \quad \text{and therefore} \quad p \equiv 1 \mod 4\,.$$

Assume now that $4 \nmid m$, $p \nmid m$ for all primes $p \equiv 3 \bmod 4$, and every proper divisor of m is already the sum of two coprime integral squares. If $m \in \{1,2\}$, there is nothing to do, and if $m = p \equiv 1 \bmod 4$ is a prime, the assertion follows by Theorem 3.2.5. Otherwise, either $m = p^k$ for some prime $p \equiv 1 \bmod 4$ and $k \ge 2$, or m is the product of two coprime smaller positive integers.

CASE 1: $m = p^k$ for some prime $p \equiv 1 \bmod 4$ and $k \ge 2$. By the induction hypothesis, $p = a^2 + b^2$ and $p^{k-1} = c^2 + d^2$, where $a,\, b,\, c,\, d \in \mathbb{Z}$, $(a,b) = 1$ and $(c,d) = 1$. Then

$$p^k = (ac - bd)^2 + (ad + bc)^2 = (ac + bd)^2 + (ad - bc)^2\,,$$

and we assert that either $(ac - bd, ad + bc) = 1$ or $(ac + bd, ad - bc) = 1$. Assume the contrary. Then p divides $ac - bd$, $ad + bc$, $ac + bd$ and $ad - bc$. Hence p also divides $(2ac, 2bd, 2ad, 2bc) = 2\big(a(c,d), b(c,d)\big) = 2(a,b)(c,d) = 2$, a contradiction.

CASE 2: $m = uv$ for some $u,\, v \in [2, m-1]$ such that $(u,v) = 1$. By the induction hypothesis, $u = a^2 + b^2$ and $v = c^2 + d^2$, where $a,\, b,\, c,\, d \in \mathbb{Z}$, $(a,b) = 1$ and $(c,d) = 1$. Then

$$uv = (ac + bd)^2 + (ad - bc)^2\,, \quad \text{and we assert that} \quad (ac + bd, ad - bc) = 1\,.$$

Assume to the contrary that there exists some prime t such that $t \,|\, ac - bd$ and $t \,|\, ad + bc$. Then t divides $c(ac + bd) + d(ad - bc) = av$, $d(ac + bd) - c(ad - bc) = bv$, $a(ac + bd) - b(ad - bc) = cu$ and $b(ac + bd) + a(ad - bc) = du$. Hence t also divides $(av, bv, cu, du) = ((a,b)v, (c,d)u) = (v,u) = 1$, a contradiction.

2. Suppose first that $m = a^2+b^2$, where $a,\, b \in \mathbb{Z}$, and set $d=(a,b)$. Then $a = da_0$, $b = db_0$ and $m = d^2m_0$, where $a_0,\, b_0 \in \mathbb{Z}$, $(a_0,b_0)=1$ and $m_0 = a_0^2+b_0^2$. If $p \equiv 3 \mod 4$ is a prime, then $p \nmid m_0$ by 1., and thus $\mathsf{v}_p(m) = 2\mathsf{v}_p(d) \equiv 0 \mod 2$.

Assume now that $2 \,|\, \mathsf{v}_p(m)$ for all primes $p \equiv 3 \mod 4$. Then there exists some $t \in \mathbb{N}$ such that $m = t^2m_0$, $p \nmid m_0$ for all primes $p \equiv 3 \mod 4$, and $4 \nmid m_0$. By 1., $m_0 = a^2+b^2$ for some $a,\, b \in \mathbb{Z}$, and therefore $m = (ta)^2+(tb)^2$.

3. Suppose that $m = 4a^2+b^2$, where $a,\, b \in \mathbb{N}$ and $(a,b)=1$. Then it follows that $m>1$, and

- if $2 \nmid b$, then $m = (2a)^2+b^2 \equiv 1 \mod 4$ and $(2a,b)=1$;
- if $2 \,|\, b$, then $b = 2b_0$, $2 \nmid a$, $(a,b_0)=1$, and therefore $m = 4m_0$, where $m_0 = a^2+b_0^2 \equiv 2 \mod 4$.

The converse is obvious. $\square$

We say that a positive integer $m \in \mathbb{N}$ has an *essentially unique* representation as a sum of two integral squares if the following assertion holds.

- If $a,\, b,\, c,\, d \in \mathbb{N}_0$ and $m = a^2+b^2 = c^2+d^2$, then $\{a,b\} = \{c,d\}$.

By the subsequent Theorem 3.4.2 every prime $p \not\equiv 3 \mod 4$ has an essentially unique representation as a sum of two integral squares. A partial converse of this assertions is the content of Exercise 3.4.3.

Theorem 3.4.2. *Let p be a prime, and suppose that*

$$p = fa^2+gb^2 = fc^2+gd^2\,,$$

where $f,\, g,\, a,\, b,\, c,\, d \in \mathbb{N}$. Then it follows that either $a=c$ and $b=d$, or $f=g=1$, $a=d$ and $b=c$. In particular, every prime $p \not\equiv 3 \mod 4$ has an essentially unique representation as a sum of two integral squares.

Proof. Since $fa^2,\, gb^2,\, fc^2,\, gd^2 \in [1,p-1]$, it follows that $p \nmid abcdfg$, and therefore there exist $u,\, v \in \mathbb{N}$ such that $bu \equiv a \bmod p$ and $dv \equiv c \bmod p$. Since $p = fa^2+gb^2 \equiv fb^2u^2+gb^2 \equiv (fu^2+g)b^2$, it follows that $fu^2+g \equiv 0 \mod p$. In the same way, $p = fc^2+gd^2$ implies $fv^2+g \equiv 0 \mod p$, hence $fu^2 \equiv fv^2 \mod p$, and thus $u \equiv \varepsilon v \mod p$ for some $\varepsilon \in \{\pm 1\}$. Since $ad - \varepsilon bc \equiv bdu - \varepsilon bdv \equiv 0 \mod p$ and $|ad-\varepsilon bc| \le ad+bc < 2p$, we obtain $ad-\varepsilon bc \in \{0, \pm p\}$.

If $ad-\varepsilon bc = 0$, then $\varepsilon = 1$, $ad = bc$, and since $(a,b)=(c,d)=1$, it follows that $a \,|\, c$ and $c \,|\, a$, hence $a=c$ and $b=d$.

If $ad-\varepsilon bc = \pm p$, then $p^2 = (fac+\varepsilon gbd)^2 + fgp^2$, hence $f=g=1$ and $ac+\varepsilon bd = 0$. We obtain $\varepsilon = -1$, $ac = bd$, and as above it follows that $a=d$ and $b=c$. $\square$

Exercise 3.4.3. Prove that a positive integer m has an essentially unique representation as a sum of two integral squares if and only if $m = 4^kc^2n$, where $k \in \mathbb{N}_0$, c is a product of primes $q \equiv 3 \mod 4$, and $n \in \{1, 2, p, 2p \mid p \in \mathbb{P}\,,\ p \equiv 1 \mod 4\}$.

Exercise 3.4.4. Prove that every positive integer which is the sum of two rational squares is already the sum of two integral squares.

Our next result deals with the arithmetical properties of a and b in the representation $p = a^2 + b^2$ of a prime p.

Theorem 3.4.5.

1. *Suppose that* $m = a^2 + b^2 \equiv 1 \bmod 4$, *where* $a,\, b \in \mathbb{N}$, $(a, b) = 1$ *and* $2 \,|\, b$. *Then it follows that* $(a, m) = (b, m) = (a + b, m) = 1$,
$$\Big(\frac{a}{m}\Big) = \Big(\frac{2b}{m}\Big) = (-1)^{(m-1)/4}\Big(\frac{b}{m}\Big) = 1 \quad \textit{and} \quad \Big(\frac{a+b}{m}\Big) = \Big(\frac{2}{a+b}\Big)\,.$$
2. *Let* $p \equiv 1 \bmod 4$ *be a prime and* $p = a^2 + b^2$, *where* $a,\, b \in \mathbb{N}$ *and* $2 \,|\, b$.
    - (a) *If* $c \in \mathbb{Z}$ *is such that* $ac \equiv b \bmod p$, *then*
    $$c^2 \equiv -1 \bmod p \quad \textit{and} \quad 2^{(p-1)/4} \equiv c^{ab/2} \bmod p\,.$$
    - (b) *If* $p \equiv 1 \bmod 8$, *then* $4 \,|\, b$, *and* 2 *is a biquadratic residue modulo* p *if and only if* $8 \,|\, b$.
3. *Let* $p \equiv 1 \bmod 8$ *be a prime. Then* 2 *is a biquadratic residue modulo* p *if and only if* $p = u^2 + 64v^2$ *for some* $u,\, v \in \mathbb{N}$.

Proof. Throughout, we tacitly apply Theorem 3.3.9.

1. Obviously, $(a, b) = 1$ implies $(a, m) = (b, m) = 1$. Since $a + b \equiv 1 \bmod 2$ and $(a+b)(a-b) + m = 2a^2$, we also get $(a+b, 2m) = 1$. For all primes p dividing a we have $m \equiv b^2 \bmod p$, and therefore

$$\Big(\frac{a}{m}\Big) = \Big(\frac{m}{a}\Big) = \prod_{p\,|\,a}\Big(\frac{m}{p}\Big)^{\mathsf{v}_p(a} = 1\,.$$

Since $(a + b)^2 = m + 2ab \equiv 2ab \bmod m$, it follows that

$$\Big(\frac{2ab}{m}\Big) = 1\,, \quad \text{and consequently} \quad \Big(\frac{2b}{m}\Big) = \Big(\frac{a}{m}\Big) = 1\,.$$

From the congruence $2m = (a + b)^2 + (a - b)^2 \equiv (a - b)^2 \bmod a + b$ it follows that

$$1 = \Big(\frac{2m}{a+b}\Big) = \Big(\frac{2}{a+b}\Big)\Big(\frac{m}{a+b}\Big) \text{ and } \Big(\frac{a+b}{m}\Big) = \Big(\frac{m}{a+b}\Big) = \Big(\frac{2}{a+b}\Big).$$

2. (a) Since $p \nmid ab$, there exists some $c \in \mathbb{Z}$ be such that $ac \equiv b \bmod p$. Then we get $a^2(1 + c^2) \equiv a^2 + b^2 \equiv 0 \bmod p$, hence $c^2 \equiv -1 \bmod p$, and

$$\Big(\frac{2}{a+b}\Big) = (-1)^{(a^2+2ab+b^2-1)/8} \equiv c^{(p-1)/4+ab/2} \bmod p\,.$$

By 1. and Euler's criterion (Theorem 3.3.1), we obtain

$$(ab)^{(p-1)/4} \equiv (a^2c)^{(p-1)/4} \equiv a^{(p-1)/2}c^{(p-1)/4} \equiv \Big(\frac{a}{p}\Big)c^{(p-1)/4} \equiv c^{(p-1)/4} \bmod p\,,$$

and since $(a + b)^2 \equiv 2ab \bmod p$, it follows that

$$\Big(\frac{2}{a+b}\Big) = \Big(\frac{a+b}{p}\Big) \equiv (a+b)^{(p-1)/2} \equiv (2ab)^{(p-1)/4} \equiv 2^{(p-1)/4}c^{(p-1)/4} \mod p\,,$$

hence $2^{(p-1)/4}c^{(p-1)/4} \equiv c^{(p-1)/4+ab/2} \bmod p$, and therefore $2^{(p-1)/4} \equiv c^{ab/2} \bmod p$.

(b) Suppose that $p \equiv 1 \bmod 8$. Then $4 \mid b$, and, by Theorem 3.1.2.1, 2 is a biquadratic residue modulo p if and only if $2^{(p-1)/4} \equiv 1 \bmod p$. Now the assertion follows by (a), since

$$2^{(p-1)/4} \equiv (c^2)^{ab/4} \equiv (-1)^{ab/4} \equiv (-1)^{b/4} \bmod p\,,$$

and therefore $2^{(p-1)/4} \equiv 1 \bmod p$ if and only if $8 \mid b$.

3. Obvious by 2. (b). □

3.5. Kronecker and quadratic symbols

Our final generalization of the Legendre symbol is the Kronecker symbol, where also the denominator is allowed to be any non-zero integer. We start with the general case, then we investigate the connection with quadratic discriminants, and in this case we call the Kronecker symbol *quadratic symbol* because of its prominent role in the more advanced theory of binary quadratic forms (Chapter 6). Throughout this section, we tacitly use the properties of the Jaobi symbol (see Theorem 3.3.9).

Let m and n be non-zero integers, and suppose that $m = 2^\beta m_1$, where $\beta \in \mathbb{N}_0$ and $m_1 \in \mathbb{Z} \setminus 2\mathbb{Z}$. We set

$$\sigma(m,n) = (-1)^{\frac{\operatorname{sgn}(m)-1}{2}\frac{\operatorname{sgn}(n)-1}{2}} = \begin{cases} -1 & \text{if} \quad m<0 \text{ and } n<0\,, \\ 1 & \text{otherwise.} \end{cases}$$

By definition, $\sigma(m,n) = \sigma(n,m)$, and if $m = m'm''$ for some $m', m'' \in \mathbb{Z}$, then $\sigma(m,n) = \sigma(m',n)\sigma(m'',n)$.

We define the *Kronecker symbol* using the Jacobi symbol by

$$\Big(\frac{n}{m}\Big) = \sigma(m,n)(-1)^{\beta(n^2-1)/8}\Big(\frac{n}{|m_1|}\Big) \quad \text{if} \quad (m,n)=1\,,$$

and

$$\Big(\frac{n}{m}\Big) = 0 \quad \text{if} \quad (n,m) \ne 1$$

(note that $(m,n)=1$ and $\beta \ne 0$ implies $n^2 \equiv 1 \bmod 8$).

If $m \in \mathbb{N}$ is odd, then the Kronecker symbol coincides with the Jacobi symbol.

Theorem 3.5.1. *Let m and n be non-zero coprime integers.*

1. *We have*

$$\Big(\frac{-1}{m}\Big) = (-1)^{(m-1)/2}\,, \qquad \Big(\frac{n}{-1}\Big) = \operatorname{sgn}(n)\,,$$

and if $2 \nmid n$, then

$$\Big(\frac{n}{2}\Big) = (-1)^{(n^2-1)/8} = \Big(\frac{2}{|n|}\Big) = \Big(\frac{2}{n}\Big)\,.$$

2. *If $m = m'm''$ and $n = n'n''$, where $m', m'', n', n'' \in \mathbb{Z}$, then*

$$\Big(\frac{n}{m}\Big) = \Big(\frac{n}{m'}\Big)\Big(\frac{n}{m''}\Big) = \Big(\frac{n'}{m}\Big)\Big(\frac{n''}{m}\Big)\,.$$

3. *Suppose that* $m = 2^\beta m_1$ *and* $n = 2^\delta n_1$, *where* $\beta,\ \delta \in \mathbb{N}_0$, $m_1,\ n_1 \in \mathbb{Z}$ *and* $2 \nmid m_1 n_1$. *Then*

$$\Big(\frac{n}{m}\Big)\Big(\frac{m}{n}\Big) = \sigma(m,n)\,(-1)^{\frac{m_1-1}{2}\,\frac{n_1-1}{2}}\,.$$

Proof. 1. We have

$$\Big(\frac{-1}{m}\Big) = \operatorname{sgn}(m)\Big(\frac{-1}{|m|}\Big) = \operatorname{sgn}(m)(-1)^{(|m|-1)/2} = (-1)^{(m-1)/2}\,.$$

The other assertions follow by the very definition.

2. Set $m' = 2^{\beta'} m_1'$ and $m'' = 2^{\beta''} m_1''$, where $\beta',\ \beta'' \in \mathbb{N}_0$, $m_1',\ m_1'' \in \mathbb{Z}$ and $2 \nmid m_1' m_1''$. Then $m = 2^{\beta'+\beta''} m_1' m_1''$, and

$$\begin{aligned}\Big(\frac{n}{m'}\Big)\Big(\frac{n}{m''}\Big) &= \sigma(m',n)\sigma(m'',n)(-1)^{(\beta'+\beta'')(n^2-1)/8)}\Big(\frac{n}{|m_1'|}\Big)\Big(\frac{n}{|m_1''|}\Big)\\ &= \sigma(m,n)(-1)^{(\beta'+\beta'')(n^2-1)/8}\Big(\frac{n}{|m_1' m_1''|}\Big) = \Big(\frac{n}{m}\Big)\,.\end{aligned}$$

If $m = 2^\beta m_1$, where $\beta \in \mathbb{Z}$, $m_1 \in \mathbb{N}$ and $2 \nmid m_1$, then

$$\begin{aligned}\Big(\frac{n'}{m}\Big)\Big(\frac{n''}{m}\Big) &= \sigma(m,n')\sigma(m,n'')(-1)^{\beta(n'^2-1/8+(n''^2-1)/8}\Big(\frac{n'}{|m_1|}\Big)\Big(\frac{n''}{|m_1|}\Big)\\ &= \sigma(m,n)\,2^{\beta(n^2-1)/8}\Big(\frac{n}{|m_1|}\Big) = \Big(\frac{n}{m}\Big)\,,\end{aligned}$$

since

$$\frac{n'^2-1}{8} + \frac{n''^2-1}{8} \equiv \frac{n^2-1}{8} \mod 2\,.$$

3. The assertion is symmetric in m and n, and as $(m,n) = 1$, we may assume that $\delta = 0$ and $n = n_1$. Then we obtain

$$\begin{aligned}\Big(\frac{n}{m}\Big)\Big(\frac{m}{n}\Big) &= \sigma(m,n)(-1)^{\beta(n^2-1)/8}\Big(\frac{n}{|m_1|}\Big)\sigma(n,m)\Big(\frac{m}{|n|}\Big) = \Big(\frac{2}{|n|}\Big)^\beta\Big(\frac{n}{|m_1|}\Big)\Big(\frac{m}{|n|}\Big)\\ &= \Big(\frac{n}{|m_1|}\Big)\Big(\frac{m_1}{|n|}\Big) = \Big(\frac{n}{|m_1|}\Big)\Big(\frac{|n|}{|m_1|}\Big)(-1)^{\frac{m_1-1}{2}\,\frac{|n|-1}{2}}\\ &= \Big(\frac{\operatorname{sgn}(n)}{|m_1|}\Big)(-1)^{\frac{m_1-1}{2}\,\frac{|n|-1}{2}} = \begin{cases}(-1)^{\frac{m_1-1}{2}\,\frac{n-1}{2}} & \text{if } n > 0\,,\\ (-1)^{\frac{|m_1|-1}{2} + \frac{m_1-1}{2}\,\frac{n+1}{2}} & \text{if } n < 0\,.\end{cases}\end{aligned}$$

If $n > 0$, we are done. If $n < 0$, then

$$\frac{|m_1|-1}{2} + \frac{m_1-1}{2}\,\frac{n+1}{2} \equiv \frac{m_1-1}{2}\,\frac{n-1}{2} \mod 2\,, \quad \text{if} \quad m > 0\,,$$

and

$$\frac{|m_1|-1}{2} + \frac{m_1-1}{2}\,\frac{n+1}{2} \equiv \frac{m_1-1}{2}\,\frac{n-1}{2} + 1 \mod 2\,, \quad \text{if} \quad m < 0\,.$$

In both cases it follows that

$$\Big(\frac{n}{m}\Big)\Big(\frac{m}{n}\Big) = \sigma(m,n)\,(-1)^{\frac{m_1-1}{2}\,\frac{n_1-1}{2}}\,. \qquad \square$$

Exercise 3.5.2. Prove that

$$\Bigl(\frac{(-1)^{(m-1)/2}m}{n}\Bigr) = \Bigl(\frac{n}{m}\Bigr)\sigma(m,n) \quad \text{if} \quad m,\, n \in \mathbb{Z} \ \text{ and } \ 2 \nmid m\,.$$

Exercise 3.5.3. Let m, n, k be non-zero integers, $2 \nmid m$, $n+km \ne 0$, $n = 2^\beta n_1$ and $n+km = 2^\gamma n_2$, where β, $\gamma \in \mathbb{N}_0$ and n_1, $n_2 \in \mathbb{Z} \setminus 2\mathbb{Z}$. Prove that

$$\Bigl(\frac{n+km}{m}\Bigr) = (-1)^{\frac{\operatorname{sgn}(m)-1}{2}\,\frac{\operatorname{sgn}(n+km)-\operatorname{sgn}(n)}{2}}\Bigl(\frac{n}{m}\Bigr)$$

and

$$\Bigl(\frac{m}{n+km}\Bigr) = (-1)^{\frac{m-1}{2}\,\frac{n_2-n_1}{2}}\Bigl(\frac{m}{n}\Bigr)\,.$$

Now we specialize the Kronecker symbol to the case where the numerator is a quadratic discriminant Δ. In this case, the Kronecker symbol turns out to be a quadratic character modulo $|\Delta|$ and even modulo a proper divisor of $|\Delta|$ unless Δ is a fundamental discriminant. To make allowance for this fact, we introduce the notion of a reduced quadratic discriminant.

Let $\Delta = \operatorname{sgn}(\Delta)\, 2^e p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ be a quadratic discriminant, where e, $r \in \mathbb{N}_0$, $e_1, \ldots, e_r \in \mathbb{N}$ and $p_1, \ldots, p_r$ are distinct odd primes. Then we define the *reduced discriminant* Δ^* associated with Δ by

$$\Delta^* = 2^{c(\Delta)} p_1 \cdot \ldots \cdot p_r\,,$$

$$\text{where} \qquad c(\Delta) \ = \ \begin{cases} 0 & \text{if} \quad \Delta \equiv 1 \bmod 4\,, \\ 1 & \text{if} \quad \Delta \equiv 4 \bmod 16\,, \\ 2 & \text{if} \quad \Delta \equiv 12 \bmod 16 \ \text{ or } \ \Delta \equiv 16 \bmod 32\,, \\ 3 & \text{if} \quad \Delta \equiv 8 \bmod 16 \ \text{ or } \ \Delta \equiv 0 \bmod 32\,. \end{cases}$$

By definition, $\Delta^* \mid \Delta$, and $\Delta^* = |\Delta|$ if and only if Δ is a fundamental discriminant. Moreover, if $n \in \mathbb{Z}$, then $(\Delta, n) = 1$ if and only if $(\Delta^*, n) = 1$.

Theorem 3.5.4. *Let Δ be a quadratic discriminant and Δ^* the associated reduced discriminant. If m and n are non-zero integers such that and $m \equiv n \bmod \Delta^*$, then*

$$\Bigl(\frac{\Delta}{m}\Bigr) = \Bigl(\frac{\Delta}{n}\Bigr)\,.$$

Proof. We set $D = \varepsilon p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$ and $\Delta = 2^e D$, where $\varepsilon = \operatorname{sgn}(\Delta)$, e, $r \in \mathbb{N}_0$, $e_1, \ldots, e_r \in \mathbb{N}$, and $p_1, \ldots, p_r$ are distinct odd primes. Then $\Delta^* = 2^{c(\Delta)} p_1 \cdot \ldots \cdot p_r$ with $c(\Delta) \in [0,3]$ as above. Let m, $n \in \mathbb{Z}^\bullet$ be such that $m \equiv n \bmod \Delta^*$. Since $m \equiv n \bmod p_i$ for all $i \in [1,r]$, we obtain

$$\Bigl(\frac{m}{|D|}\Bigr) = \Bigl(\frac{n}{|D|}\Bigr), \quad \text{hence} \quad \Bigl(\frac{m}{|D|}\Bigr)\Bigl(\frac{n}{|D|}\Bigr) = 1\,, \quad \text{and we assert that} \quad \Bigl(\frac{\Delta}{m}\Bigr)\Bigl(\frac{\Delta}{n}\Bigr) = 1\,.$$

We set $m = 2^\beta m_1$ and $n = 2^\delta n_1$, where $\beta,\ \delta \in \mathbb{N}_0,\ \ \beta \le \delta$ and $m_1,\ n_1 \in \mathbb{Z} \setminus 2\mathbb{Z}$. We may assume that $(\Delta, m) = 1$, hence $(\Delta, n) = (\Delta^*, n) = (\Delta^*, m) = 1$, and we obtain

$$\begin{aligned}\Big(\frac{\Delta}{m}\Big)\Big(\frac{\Delta}{n}\Big) &= \sigma(m,\Delta)\sigma(n,\Delta)(-1)^{(\beta+\delta)/(\Delta^2-1)/8}\Big(\frac{2}{|m_1|}\Big)^e\Big(\frac{D}{|m_1|}\Big)\Big(\frac{2}{|n_1|}\Big)^e\Big(\frac{D}{|n_1|}\Big)\\ &= \sigma(mn,\Delta)(-1)^{(\beta+\delta)/(\Delta^2-1)/8}\Big(\frac{2}{m_1n_1}\Big)^e\Big(\frac{|m_1|}{|D|}\Big)\Big(\frac{|n_1|}{|D|}\Big)(-1)^{\frac{D-1}{2}\left(\frac{|m_1|-1}{2}+\frac{|n_1|-1}{2}\right)}\\ &= \sigma(mn,\Delta)(-1)^{(\beta+\delta)/(\Delta^2-1)/8}\Big(\frac{2}{m_1n_1}\Big)^e\Big(\frac{\operatorname{sgn}(mn)}{|D|}\Big)(-1)^{\frac{D-1}{2}\left(\frac{|m_1|-1}{2}+\frac{|n_1|-1}{2}\right)}\,.\end{aligned}$$

CASE 1: $\Delta \equiv 1 \bmod 4$. Then $e = 0,\ \ D = \Delta$, and

$$\Big(\frac{\Delta}{m}\Big)\Big(\frac{\Delta}{n}\Big) = \sigma(mn,\Delta)\Big(\frac{\operatorname{sgn}(mn)}{|\Delta|}\Big) = 1\,.$$

CASE 2: $\Delta \equiv 0 \bmod 4$. Then $\beta = \delta = 0,\ \ m_1 = m,\ \ n_1 = n$, and

$$\Big(\frac{\Delta}{m}\Big)\Big(\frac{\Delta}{n}\Big) = \sigma(mn,\Delta)\Big(\frac{\operatorname{sgn}(mn)}{|D|}\Big)\Big(\frac{2}{mn}\Big)^e(-1)^{\frac{D-1}{2}\left(\frac{|m|-1}{2}+\frac{|n|-1}{2}\right)}\,.$$

If $\Delta \equiv 4 \bmod 16$, then $e = 2,\ \ D \equiv 1 \bmod 4$, and we obtain

$$\Big(\frac{\Delta}{m}\Big)\Big(\frac{\Delta}{n}\Big) = \sigma(mn,D)\Big(\frac{\operatorname{sgn}(mn)}{|D|}\Big) = 1\,.$$

If $\Delta \not\equiv 4 \bmod 16$, then $c(\Delta) \ge 2,\ \ m \equiv n \bmod 4$, and we assert that

$$\sigma(mn,D)\Big(\frac{\operatorname{sgn}(mn)}{|D|}\Big)(-1)^{\frac{D-1}{2}\left(\frac{|m|-1}{2}+\frac{|n|-1}{2}\right)} = 1\,, \quad \text{hence} \quad \Big(\frac{\Delta}{m}\Big)\Big(\frac{\Delta}{n}\Big) = \Big(\frac{2}{mn}\Big)^e.$$

Indeed, if $mn > 0$, then

$$\sigma(mn,D)\Big(\frac{\operatorname{sgn}(mn)}{|D|}\Big)(-1)^{\frac{D-1}{2}\left(\frac{|m|-1}{2}+\frac{|n|-1}{2}\right)} = (-1)^{\frac{D-1}{2}\,\frac{m+n-2}{2}} = 1\,,$$

and if $mn < 0$, then

$$\sigma(mn,D)\Big(\frac{\operatorname{sgn}(mn)}{|D|}\Big)(-1)^{\frac{D-1}{2}\left(\frac{|m|-1}{2}+\frac{|n|-1}{2}\right)} = \operatorname{sgn}(D)\Big(\frac{-1}{|D|}\Big)(-1)^{(D-1)/2} = 1\,.$$

If $\Delta \equiv 12 \bmod 16$ or $\Delta \equiv 16 \bmod 32$, then $e \equiv 0 \bmod 2$, and we are done. In all other cases, $c(\Delta) \ge 3$ and $m \equiv n \bmod 8$, hence $mn \equiv 1 \bmod 8$, and we are done, too. □

Let now Δ be a quadratic discriminant and Δ^* the associated reduced discriminant. By the Theorems 3.5.1 and 3.5.4, the Kronecker symbol induces a character $\mathsf{Q}_\Delta \in \mathsf{X}(\Delta^*)$ such that

$$\mathsf{Q}_\Delta(a + \Delta^*\mathbb{Z}) = \Big(\frac{\Delta}{a}\Big) \quad \text{for all} \quad a \in \mathbb{Z} \ \text{ such that } \ (\Delta, a) = 1\,.$$

The character $\mathsf{Q}_\Delta \colon (\mathbb{Z}/\Delta^*\mathbb{Z})^\times \to \{\pm 1\}$ is called the *quadratic symbol* associated with Δ. According to the conventions made in Section 3.2, we also view Q_Δ as a Dirirchlet character modulo Δ^*. Under this aspect, it is function

$$\mathsf{Q}_\Delta \colon \mathbb{Z} \to \{0, \pm 1\}$$

such that the following assertions hold for all $a,\ b \in \mathbb{Z}$:

- $\mathsf{Q}_\Delta(a)=0$ if and only if $(\Delta,a)\neq 1$.
- $\mathsf{Q}_\Delta(ab)=\mathsf{Q}_\Delta(a)\mathsf{Q}_\Delta(b)$.
- $\mathsf{Q}_\Delta(a)=\mathsf{Q}_\Delta(b)$ if $a\equiv b \bmod \Delta^*$.

In the following two theorems, we investigate the properties of the quadratic symbol in detail. Then we calculate the Gauss sum $\tau(\mathsf{Q}_\Delta)$ for fundamental discriminants Δ (Theorems 3.5.7 and 3.5.8), and we close this section with an explicit description of the group of all real characters modulo m for an arbitrary modulus (Theorem 3.5.10).

Theorem 3.5.5. *Let Δ be a quadratic discriminant and Δ^* the associated reduced discriminant.*

1. $\mathsf{Q}_\Delta\in\mathsf{X}(\Delta^*)$ *is a quadratic character,*

$$\mathsf{Q}_\Delta(-1)=\operatorname{sgn}(\Delta)\,,\quad \textit{and if}\ \ \Delta\equiv 1 \bmod 4,\ \textit{then}\quad \mathsf{Q}_\Delta(2)=(-1)^{(\Delta-1)/4}\,.$$

2. *Suppose that $a\in\mathbb{Z}$ and $(\Delta,a)=1$.*
   (a) *If $\Delta\equiv 1 \bmod 4$, then*

$$\mathsf{Q}_\Delta(a)=\Bigl(\frac{a}{|\Delta|}\Bigr)\,.$$

In particular, if $\Delta=(-1)^{(p-1)/2}p$ for some odd prime p, then $\mathsf{Q}_\Delta=\varphi_p$ is the unique quadratic character modulo p, and

$$\mathsf{Q}_\Delta(a)=\Bigl(\frac{a}{p}\Bigr)\,.$$

   (b) *Suppose that $\Delta=2^eD$, where $e\geq 2$, $D\in\mathbb{Z}$ and $2\nmid D$. Then*

$$\mathsf{Q}_\Delta(a)=(-1)^{e(a^2-1)/8+\frac{a-1}{2}\frac{D-1}{2}}\Bigl(\frac{a}{|D|}\Bigr)\,,$$

$$\mathsf{Q}_{-4}(a)=\Bigl(\frac{-1}{a}\Bigr)\,,\quad \mathsf{Q}_{8}(a)=\Bigl(\frac{2}{a}\Bigr)\,,\quad \mathsf{Q}_{-8}(a)=\Bigl(\frac{-2}{a}\Bigr)\,,$$

and

$$\mathsf{Q}_\Delta\Bigl(a\pm\frac{\Delta}{2}\Bigr)=\begin{cases}-\mathsf{Q}_\Delta(a) & \textit{if either}\ \ e=3\ \ \textit{or}\ \ e=2,\ D\equiv 3 \bmod 4\,,\\ \mathsf{Q}_\Delta(a) & \textit{otherwise}\,.\end{cases}$$

3. *If $m\in\mathbb{Z}$, $(\Delta,m)=1$, and Δ is a quadratic residue modulo $4|m|$, then*

$$\mathsf{Q}_\Delta(m)=\sigma(m,\Delta)=\begin{cases}-1 & \textit{if}\quad \Delta<0\quad \textit{and}\quad m<0\,,\\ 1 & \textit{otherwise.}\end{cases}$$

4. *If p is a prime, then Δ is a quadratic residue modulo $4p$ if and only if $\mathsf{Q}_\Delta(p)\neq -1$.*

Proof. 1. By definition, we have $\mathsf{Q}_\Delta(-1)=\operatorname{sgn}(\Delta)$, and $\mathsf{Q}_\Delta(2)=(-1)^{(\Delta-1)/4}$ if $\Delta\equiv 1 \bmod 4$.

It remains to prove that also for $\Delta>0$ there exists some $k\in\mathbb{Z}$ such that $\mathsf{Q}_\Delta(k)=-1$. Suppose that $\Delta=2^ed$, where $e\in\mathbb{N}_0$, $d\in\mathbb{N}$ and $2\nmid d$.

CASE 1: d is not a square. Then $d = p^{2l+1}d_0$ for some odd prime p, $l \in \mathbb{N}_0$, $d_0 \in \mathbb{N}$ and $p \nmid d_0$. Let $k \in \mathbb{N}$ be such that $k \equiv 1 \bmod 8d_0$, and k is a quadratic non-residue modulo p. Then

$$\mathsf{Q}_\Delta(k) = \Big(\frac{\Delta}{k}\Big) = \Big(\frac{2^e p d_0}{k}\Big) = \Big(\frac{2}{k}\Big)^e \Big(\frac{k}{p}\Big)\Big(\frac{k}{d_0}\Big) = \Big(\frac{k}{p}\Big) = -1\,.$$

CASE 2: d is a square. Since $\Delta > 0$, it follows that e is odd, and therefore

$$\mathsf{Q}_\Delta(5) = \Big(\frac{\Delta}{5}\Big) = \Big(\frac{2^e}{5}\Big) = \Big(\frac{2}{5}\Big) = -1\,.$$

2. Suppose that $\Delta = 2^e D$, where $e \in \mathbb{N}_0$, $D \in \mathbb{Z} \setminus 2\mathbb{Z}$ and $a = 2^\beta a_1$, where $\beta \in \mathbb{N}_0$ and $a_1 \in \mathbb{Z} \setminus 2\mathbb{Z}$. Then we obtain

$$\begin{aligned}\mathsf{Q}_\Delta(a) = \Big(\frac{\Delta}{a}\Big) &= \sigma(a,\Delta)(-1)^{\beta(\Delta^2-1)/8}\Big(\frac{2}{|a_1|}\Big)^e\Big(\frac{D}{|a_1|}\Big) \\ &= \sigma(a,\Delta)(-1)^{\beta(\Delta^2-1)/8+e(a_1^2-1)/8}\Big(\frac{|a_1|}{|D|}\Big)(-1)^{\frac{|a_1|-1}{2}\frac{D-1}{2}}\,.\end{aligned}$$

CASE 1: $\Delta \equiv 1 \bmod 4$. Then $\Delta = D$, $e = 0$, and

$$\mathsf{Q}_\Delta(a) = \sigma(a,\Delta)\Big(\frac{2}{|\Delta|}\Big)^\beta\Big(\frac{|a_1|}{|\Delta|}\Big) = \sigma(a,\Delta)\Big(\frac{\operatorname{sgn}(a)}{|\Delta|}\Big)\Big(\frac{a}{|\Delta|}\Big) = \Big(\frac{a}{|\Delta|}\Big)\,.$$

CASE 2: $\Delta \equiv 0 \bmod 4$. Then $\beta = 0$, $a_1 = a$, and

$$\mathsf{Q}_\Delta(a) = \sigma(a,D)(-1)^{e(a^2-1)/8+\frac{|a|-1}{2}\frac{D-1}{2}}\Big(\frac{\operatorname{sgn}(a)}{|D|}\Big)\Big(\frac{a}{|D|}\Big)\,.$$

Hence we must prove that

$$\sigma(a,D)\Big(\frac{\operatorname{sgn}(a)}{|D|}\Big)(-1)^{\frac{|a|-1}{2}\frac{D-1}{2}} = (-1)^{\frac{a-1}{2}\frac{D-1}{2}}\,.$$

This is obvious if $a > 0$, and if $a < 0$, then

$$\sigma(a,D)\Big(\frac{\operatorname{sgn}(a)}{|D|}\Big)(-1)^{\frac{|a|-1}{2}\frac{D-1}{2}} = \begin{cases} (-1)^{\frac{D-1}{2}+\frac{a+1}{2}\frac{D-1}{2}} = (-1)^{\frac{a-1}{2}\frac{D-1}{2}} & \text{if } D > 0\,, \\ -(-1)^{\frac{D+1}{2}+\frac{a+1}{2}\frac{D-1}{2}} = (-1)^{\frac{a-1}{2}\frac{D-1}{2}} & \text{if } D < 0\,. \end{cases}$$

Next we consider the three special discriminants.

- $\Delta = -4$: $e = 2$, $D = -1$, and if $a \in \mathbb{Z} \setminus 2\mathbb{Z}$, then
$$Q_{-4}(a) = (-1)^{(a-1)/2} = \Big(\frac{-1}{a}\Big)\,.$$
- $\Delta = 8$: $e = 3$, $D = 1$, and if $a \in \mathbb{Z} \setminus 2\mathbb{Z}$, then
$$Q_8(a) = (-1)^{(a^2-1)/8} = \Big(\frac{2}{a}\Big)\,.$$
- $\Delta = -8$: $e = 3$, $D = -1$, and if $a \in \mathbb{Z} \setminus 2\mathbb{Z}$, then
$$Q_{-8}(a) = (-1)^{(a^2-1)/8+(a-1)/2} = \Big(\frac{2}{a}\Big)\Big(\frac{-1}{a}\Big) = \Big(\frac{-2}{a}\Big)\,.$$

Finally, if $e \ge 2$, then

$$\frac{(a \pm 2^{e-1}D)^2-1}{8} = \frac{a^2-1}{8} \pm \frac{2^e aD + 2^{2e-2}D^2}{8}\,,$$

$$\frac{(a \pm 2^{e-1}D-1)}{2}\,\frac{D-1}{2} = \frac{a-1}{2}\,\frac{D-1}{2} \pm \frac{2^{e-1}D(D-1)}{4}\,,$$

and therefore

$$\mathsf{Q}_\Delta\Big(a+\frac{\Delta}{2}\Big) = \mathsf{Q}_\Delta(a+2^{e-1}D) = \mathsf{Q}_\Delta(a)(-1)^E\,,$$

where

$$E = \frac{e(2^e aD + 2^{2e-2}D^2)}{8} + \frac{2^{e-1}D(D-1)}{4} = \frac{2^eD(ae+2^{e-2}eD+D-1)}{8}\,.$$

Now the assertion follows since

$$2^eD(ae+2^{e-2}eD+D-1) \equiv \begin{cases} 8 \bmod 16 & \text{if either } e=3 \text{ or } e=2,\;\; D\equiv 3 \bmod 4, \\ 0 \bmod 16 & \text{otherwise.} \end{cases}$$

3. Suppose that $m = 2^\beta m_1$, where $\beta \in \mathbb{N}_0$ and $m_1 \in \mathbb{Z}\setminus 2\mathbb{Z}$. If Δ is a quadratic residue modulo $4|m|$, then Δ is a quadratic residue modulo p for each prime p dividing m_1, hence

$$\mathsf{Q}_\Delta(m) = \Big(\frac{\Delta}{m}\Big) = \sigma(m,\Delta)(-1)^{\beta(\Delta^2-1)/8}\Big(\frac{\Delta}{|m_1|}\Big) = \sigma(m,\Delta)(-1)^{\beta(\Delta-1)/4}\,.$$

If $\beta = 0$, there is nothing to do. If $\beta > 0$, then $4m \equiv 0 \bmod 8$, $\Delta \equiv 1 \bmod 4$, and Δ is a quadratic residue modulo 8. Hence $\Delta \equiv 1 \bmod 8$, and again the assertion follows.

4. CASE 1: $p \nmid \Delta$. Then

$$\mathsf{Q}_\Delta(p) = \Big(\frac{\Delta}{p}\Big) \quad \text{by the very definition.}$$

If $p \ne 2$, then $\mathsf{Q}_\Delta(p) = 1$ if and only if Δ is a quadratic residue modulo p, and as $\Delta \equiv 0$ or $1 \bmod 4$, this holds if and only if Δ is a quadratic residue modulo $4p$.

If $p = 2$, then $\mathsf{Q}_\Delta(p) = 1$ if and only if $\Delta \equiv 1 \bmod 8$, that is, if and only if Δ is a quadratic residue modulo 8.

CASE 2: $p \mid \Delta$. If $p \ne 2$, then Δ is a quadratic residue modulo p, and as Δ is a quadratic residue modulo 4, it follows that Δ is a quadratic residue modulo $4p$. If $p = 2$, then $\Delta \equiv 0$ or $4 \bmod 8$, and thus Δ is a quadratic residue modulo 8. □

Theorem 3.5.6. *Let* $\Delta = 2^eD$ *be a quadratic discriminant, where* $e \in \mathbb{N}_0$, $D \in \mathbb{Z}$ *and* $|D| = p_1^{e_1}\cdot\ldots\cdot p_r^{e_r}$ *with* $r \in \mathbb{N}_0$, $e_1,\ldots,e_r \in \mathbb{N}$ *and distinct odd primes* $p_1,\ldots,p_r$. *Let* Δ^* *be the reduced discriminant associated with* Δ. *Then* Q_Δ *is a primitive character modulo* Δ^* *if and only if* $2 \nmid e_i$ *for all* $i \in [1,r]$, *and one of the following conditions is fulfilled*:

- $e = 0$.
- $2 \nmid e$.
- $2 \mid e$ *and* $D \equiv 3 \bmod 4$.

In particular, if Δ *is a fundamental discriminant, then* $\Delta^* = |\Delta|$, *and* Q_Δ *is a primitive character modulo* $|\Delta|$.

Proof. Let $c = c(\Delta) \in [0,3]$ be such that $\Delta^* = 2^c p_1 \cdot \ldots \cdot p_r$. By Theorem 3.2.1.1, Q_Δ is primitive if and only if for every proper positive divisor k of Δ^* there exists some $a \in \mathbb{Z}$ such that $a \equiv 1 \mod k$ and $\mathsf{Q}_\Delta(a) = -1$.

CASE 1: $2 \,|\, e_i$ for some $i \in [1,r]$, say $2 \,|\, e_r$. We set $k = 2^c p_1 \cdot \ldots \cdot p_{r-1}$, and we assert that $\mathsf{Q}_\Delta(a) = 1$ for all $a \in \mathbb{Z}$ satisfying $(\Delta, a) = 1$ and $a \equiv 1 \mod k$.

Thus assume that $a \in \mathbb{Z}$, $(\Delta, a) = 1$ and $a \equiv 1 \mod k$. Then

$$\Big(\frac{a}{|D|}\Big) = \prod_{i=1}^{r} \Big(\frac{a}{p_i}\Big)^{e_i} = \Big(\frac{a}{p_r}\Big)^{e_r} = 1\,,$$

and if $\Delta \equiv 1 \mod 4$, then $\mathsf{Q}_\Delta(a) = 1$.

If $\Delta \equiv 0 \mod 4$,then we obtain $\mathsf{Q}_\Delta(a) = (-1)^{e(a^2-1)/8 + \frac{a-1}{2}\frac{D-1}{2}}$, and we must consider the different possible cases.

If $\Delta \equiv 4 \mod 16$, then $e = 2$ and $D \equiv 1 \mod 4$, hence $\mathsf{Q}_\Delta(a) = 1$.

If $\Delta \equiv 12 \mod 16$ or $\Delta \equiv 16 \mod 32$, then $2 \,|\, e$ and $c = 2$, hence $a \equiv 1 \mod 4$ and thus $\mathsf{Q}_\Delta(a) = 1$.

If $\Delta \equiv 8 \mod 16$ or $\Delta \equiv 0 \mod 32$, then $c = 3$, hence $a \equiv 1 \mod 8$, and again $\mathsf{Q}_\Delta(a) = 1$.

CASE 2: $2 \nmid e_i$ for all $i \in [1,r]$. We prove first:

A. If $k \,|\, \Delta^*$ and $p_1 \cdot \ldots \cdot p_r \nmid k$, then there exists some $a \in \mathbb{Z}$ such that $(\Delta, a) = 1$, $a \equiv 1 \mod k$, and $\mathsf{Q}_\Delta(a) = -1$.

Proof of **A.** Suppose that $k \,|\, \Delta^*$ and $p_r \nmid k$. Let $a \in \mathbb{N}$ be such that

$$a \equiv 1 \mod 8p_1 \cdot \ldots \cdot p_{r-1} \quad \text{and} \quad \Big(\frac{a}{p_r}\Big) = -1.$$

Then $a \equiv 1 \mod k$, and we obtain (regardless of $\Delta \equiv 1$ or $0 \mod 4$)

$$\mathsf{Q}_\Delta(a) = (-1)^{e(a^2-1)/8 + \frac{a-1}{2}\frac{D-1}{2}} \Big(\frac{a}{|D|}\Big) = \prod_{i=1}^{r} \Big(\frac{a}{p_i}\Big)^{e_i} = \Big(\frac{a}{p_r}\Big)^{e_r} = -1. \quad \square[\mathbf{A}.]$$

Using **A**, we get the following criterion:

> Q_Δ is primitive if and only if, for every $\gamma \in [0, c-1]$ there is some $a \in \mathbb{Z}$ satisfying $(\Delta, a) = 1$ and $a \equiv 1 \mod 2^\gamma p_1 \cdot \ldots \cdot p_r$ such that $\mathsf{Q}_\Delta(a) = -1$.

In particular, it follows that Q_Δ is primitive if $e = 0$.

Assume now that $e \geq 2$. If $\gamma \in [0, c-1]$ and $a \in \mathbb{Z}$ is such that $(\Delta, a) = 1$ and $a \equiv 1 \mod 2^\gamma p_1 \cdot \ldots \cdot p_r$, then (as above)

$$\mathsf{Q}_\Delta(a) = (-1)^{e(a^2-1)/8 + \frac{a-1}{2}\frac{D-1}{2}}\,.$$

If $2 \,|\, e$ and $D \equiv 1 \mod 4$, then $\mathsf{Q}_\Delta(a) = 1$ whenever $a \equiv 1 \mod p_1 \cdot \ldots \cdot p_r$, and thus Q_Δ is not primitive.

If $2 \nmid e$ and $\gamma \in [0, c-1]$, then $\gamma \leq 2$, and there exists some $a \in \mathbb{Z}$ such that $a \equiv 1 \mod 2^\gamma p_1 \cdot \ldots \cdot p_r$ and $a \equiv 5 \mod 8$, which implies $\mathsf{Q}_\Delta(a) = -1$. Hence Q_Δ is primitive.

If $2 \,|\, e$ and $D \equiv 3 \mod 4$, then $c = 2$. If $\gamma \leq 1$, then exists some $a \in \mathbb{Z}$ such that $a \equiv 1 \mod 2^\gamma p_1 \cdot \ldots \cdot p_r$ and $a \equiv 3 \mod 4$, which implies $\mathsf{Q}_\Delta(a) = -1$. Hence Q_Δ is primitive also in this case. $\square$

To calculate the Gauss sum $\tau(\mathsf{Q}_\Delta)$, we consider first the case of a prime discriminant $\Delta = (-1)^{(p-1)/2}p$ for an odd prime p. In this case, $\mathsf{Q}_\Delta = \varphi_p$ is the unique quadratic character modulo p.

Theorem 3.5.7. *Let p be an odd prime and $\varphi_p \in \mathsf{X}(p)$ the unique quadratic character modulo p. Then*

$$\tau(\varphi_p) = \begin{cases} \sqrt{p} & \text{if} \quad p \equiv 1 \mod 4\,, \\ \mathsf{i}\sqrt{p} & \text{if} \quad p \equiv 3 \mod 4\,. \end{cases}$$

Proof. There exist several proofs of this famous theorem of Gauss, both analytic and algebraic. We refer to [**6**] for an overview. Here we present an algebraic proof due to W. C. Waterhouse [**106**].

Since $\varphi_p \in \mathsf{X}(p)$ is primitive and $\overline{\varphi}_p = \varphi_p$, Theorem 3.2.1.3 implies $\tau(\varphi_p) = \varepsilon\sqrt{p}$, where $\varepsilon \in \mathbb{C}$ and $|\varepsilon| = 1$. We must prove that

$$\varepsilon = \begin{cases} 1 & \text{if} \quad p \equiv 1 \mod 4\,, \\ \mathsf{i} & \text{if} \quad p \equiv 3 \mod 4\,. \end{cases}$$

Let V be the complex vector space of all functions $\mathbb{F}_p^\times \to \mathbb{C}$ (with point-wise composition). For $\nu \in \mathbb{F}_p^\times$ let $\mathsf{e}_\nu \in V$ be defined by $\mathsf{e}_\nu(\mu) = \delta_{\nu,\mu}$ for all $\mu \in \mathbb{F}_p^\times$. Then $(\mathsf{e}_\nu)_{\nu\in\mathbb{F}_p^\times}$ is a $\mathbb{C}$-basis of V, and $\dim_\mathbb{C}(V) = p-1$.

We fix some $\omega \in \mathbb{F}_p^\times$ such that $\mathbb{F}_p^\times = \langle\omega\rangle$ and denote by $\chi \in \mathsf{X}(p)$ the unique character satisfying $\chi(\omega) = \zeta_{p-1}$. Then $\chi(-1) = \chi(\omega^{(p-1)/2}) = \zeta_{p-1}^{(p-1)/2} = -1$, $\mathsf{X}(p) = \langle\chi\rangle$, and we assert that $\{\chi^\nu \mid \nu \in [0, p-2]\}$ is also a basis of V. For this, it suffices to prove that $\{\chi^\nu \mid \nu \in [0, p-2]\}$ is linearly independent over $\mathbb{C}$. Let $(a_\nu)_{\nu\in[0,p-2]}$ be a sequence in $\mathbb{C}$ satisfying

$$\sum_{\nu=0}^{p-2} a_\nu\chi^\nu = 0\,, \quad \text{and thus} \quad \sum_{\nu=0}^{p-2} a_\nu\chi^\nu(\omega^\mu) = \sum_{\nu=0}^{p-2} a_\nu\zeta_{p-1}^{\nu\mu} = 0 \quad \text{for all} \quad \mu \in [0, p-2]\,.$$

Since $\det(\zeta_{p-1}^{\nu\mu})_{\nu,\mu[0,p-2]} \neq 0$ (it is a Vandermonde determinant), we obtain $a_\nu = 0$ for all $\nu \in [0, p-2]$.

Now we define $\Theta\colon V \to V$ by

$$\Theta(f)(n) = \sum_{\nu\in\mathbb{F}_p^\times} f(\nu)\zeta_p^{n\nu} \quad \text{for all} \quad f \in V \quad \text{and} \quad n \in \mathbb{F}_p^\times\,.$$

Θ is $\mathbb{C}$-linear, and we shall calculate its determinant twice, first using the basis $(\mathsf{e}_\nu)_{\nu\in\mathbb{F}_p^\times}$, and then using the basis $(\chi^\nu)_{\nu\in[0,p-2]}$.

For j, $n \in \mathbb{F}_p^\times$, we have

$$\Theta(\mathsf{e}_j)(n) = \sum_{\nu\in\mathbb{F}_p^\times} \mathsf{e}_j(\nu)\zeta_p^{n\nu} = \Big(\sum_{\nu\in\mathbb{F}_p^\times} \zeta_p^{\nu j}\mathsf{e}_\nu\Big)(n)\,, \quad \text{hence} \quad \Theta(\mathsf{e}_j) = \sum_{\nu\in\mathbb{F}_p^\times} \zeta_p^{\nu j}\mathsf{e}_\nu\,,$$

and therefore, by Lemma A.7.2,

$$\det(\Theta) = \det(\zeta_p^{\nu j})_{\nu,j\in\mathbb{F}_p^\times} = \det(\zeta_p^{\nu\mu})_{\nu,\,\mu\in[0,p-2]} = \mathsf{i}^{p(p-1)/2}b_0 \quad \text{for some} \quad b_0 \in R_{>0}\,.$$

To calculate $\det(\Theta)$ using the basis $(\chi^j)_{j\in[0,p-2]}$, we decompose V into Θ-invariant subspaces. For $n \in \mathbb{F}_p^\times$, we obtain

$$\Theta(\mathbf{1}_p)(n) = \sum_{\nu\in\mathbb{F}_p^\times} \zeta_p^{n\nu} = \sum_{\nu\in\mathbb{F}_p} \zeta_p^{n\nu} - 1 = -1 = (-\mathbf{1}_p)(n)\,,$$

$$\Theta(\varphi_p)(n) = \sum_{\nu\in\mathbb{F}_p^\times} \varphi_p(\nu)\zeta_p^{n\nu} = \tau(\varphi_p, n) = \varphi_p(n)\tau(\varphi_p) = [\tau(\varphi_p)\varphi_p](n)\,,$$

and, for all $j \in [1, (p-3)/2]$,

$$\Theta(\chi^{\pm j})(n) = \sum_{\nu\in\mathbb{F}_p^\times} \chi^{\pm j}(\nu)\zeta_p^{n\nu} = \tau(\chi^{\pm j}, n) = \chi^{\mp j}(n)\tau(\chi^{\pm j}) = [\tau(\chi^{\pm j})\chi^{\mp j}](n)\,.$$

Hence we have the decomposition

$$V = \mathbb{C}\mathbf{1}_p \oplus \mathbb{C}\varphi_p \oplus \bigoplus_{j=1}^{(p-3)/2} V_j\,, \quad \text{where} \;\; V_j = \mathbb{C}\chi^j + \mathbb{C}\chi^{-j} \;\; \text{for all} \;\; j \in \Big[1, \frac{p-3}{2}\Big]\,.$$

The action of Θ on the Θ-invariant direct summands is given by $\Theta(\mathbf{1}_p) = -\mathbf{1}_p$, $\Theta(\varphi_p) = \tau(\varphi_p)\varphi_p$, and

$$\big(\Theta(\chi^j),\, \Theta(\chi^{-j}) = \big(\chi^j,\, \chi^{-j}\big)\begin{pmatrix} 0 & \tau(\chi^{-j}) \\ \tau(\chi^j) & 0 \end{pmatrix} \quad \text{for all} \;\; j \in \Big[1, \frac{p-3}{2}\Big]\,.$$

Thus we get $\det(\Theta \,|\, \mathbb{C}\mathbf{1}_p) = -1$, $\det(\Theta \,|\, \mathbb{C}\varphi_p) = \tau(\varphi_p)$, and (using Theorem 3.2.1.3) $\det(\Theta \,|\, V_j) = -\tau(\chi^j)\tau(\chi^{-j}) = -\chi^j(-1)p = (-1)^{j+1}p$. Putting this information together, it follows that

$$\begin{aligned} \det(\Theta) &= \det(\Theta \,|\, \mathbb{C}\mathbf{1}_p)\, \det(\Theta \,|\, \mathbb{C}\varphi_p) \prod_{j=1}^{(p-3)/2} \det(\Theta \,|\, V_j) = -\tau(\varphi_p) \prod_{j=1}^{(p-3)/2} [(-1)^{j+1}p] \\ &= (-1)^{1+2+\ldots+((p-1)/2}\tau(\varphi_p)p^{(p-3)/2} = (-1)^{(p^2-1)/8}\tau(\varphi_p)p^{(p-3)/2} \\ &= (-1)^{(p^2-1)/8}\varepsilon b_1 \quad \text{for some} \;\; b_1 \in \mathbb{R}_{>0}\,. \end{aligned}$$

We compare the two results and obtain

$$\varepsilon = \mathsf{i}^{p(p-1)/2-(p^2-1)/4} = \mathsf{i}^{(p-1)^2/4} = \begin{cases} 1 & \text{if} \quad p \equiv 1 \mod 4\,, \\ \mathsf{i} & \text{if} \quad p \equiv 3 \mod 4\,. \end{cases}$$

□

Theorem 3.5.8. *Let* Δ *be a fundamental discriminant. Then* $\tau(\mathsf{Q}_\Delta) = \sqrt{\Delta}$.

$$\tau(\mathsf{Q}_\Delta) = \sqrt{\Delta} = \begin{cases} \sqrt{\Delta} & \textit{if} \quad \Delta > 0\,, \\ \mathsf{i}\sqrt{|\Delta|} & \textit{if} \quad \Delta < 0\,. \end{cases}$$

Proof. We use induction on the number of prime factors of Δ. The main difficulty arises for odd prime discriminants, and this case was already done in Theorem 3.5.7.

CASE 1: Δ is a prime discriminant. If $\Delta=(-1)^{(p-1)/2}p$ for some odd prime p, then $\mathsf{Q}_\Delta=\varphi_p$, and the assertion holds by Theorem 3.5.7. It remains to consider the discriminants $\Delta\in\{-4,\ \pm8\}$. Simple calculations show that

$$\tau(\mathsf{Q}_{-4})=\mathsf{Q}_{-4}(1)\,\mathsf{i}+\mathsf{Q}_{-4}(3)\,\mathsf{i}^3=2\mathsf{i}=\sqrt{-4}\,,$$

$$\tau(\mathsf{Q}_8)=\mathsf{Q}_8(1)\zeta_8+\mathsf{Q}_8(3)\zeta_8^3+\mathsf{Q}_8(5)\zeta_8^5+\mathsf{Q}_8(7)\zeta_8^7=\zeta_8-\zeta_8^3-\zeta_8^5+\zeta_8^7=2\zeta_8(1-\mathsf{i})=\sqrt{8}$$

and

$$\begin{aligned}\tau(\mathsf{Q}_{-8})&=\mathsf{Q}_{-8}(1)\zeta_8+\mathsf{Q}_{-8}(3)\zeta_8^3+\mathsf{Q}_{-8}(5)\zeta_8^5+\mathsf{Q}_{-8}(7)\zeta_8^7=\zeta_8+\zeta_8^3-\zeta_8^5-\zeta_8^7\\&=2\zeta_8(1+\mathsf{i})=\sqrt{-8}\,.\end{aligned}$$

CASE 2: Δ is not a prime discriminant. It suffices to prove:

A. There exists a factorization $\Delta=\Delta_1\Delta_2$ into fundamental discriminants Δ_1, Δ_2 such that $(\Delta_1,\Delta_2)=1$, and for each such factorization we have

$$\tau(\mathsf{Q}_\Delta)=\begin{cases}-\tau(\mathsf{Q}_{\Delta_1})\tau(\mathsf{Q}_{\Delta_2}) & \text{if}\quad \Delta_1<0\ \text{ and }\ \Delta_2<0\,,\\ \tau(\mathsf{Q}_{\Delta_1})\tau(\mathsf{Q}_{\Delta_2}) & \text{otherwise}\,.\end{cases}$$

Indeed, suppose that **A** holds, and let $\Delta=\Delta_1\Delta_2$ be a factorization into fundamental discriminants Δ_1, Δ_2 such that $(\Delta_1,\Delta_2)=1$. Then $\tau(\mathsf{Q}_{\Delta_i})=\sqrt{\Delta_i}$ for $i\in\{1,2\}$ by the induction hypothesis, and it follows that $\tau(\mathsf{Q}_\Delta)=\sqrt{\Delta}$, since

$$\tau(\mathsf{Q}_{\Delta_1})\tau(\mathsf{Q}_{\Delta_2})=\sqrt{\Delta_1}\sqrt{\Delta_2}=\begin{cases}-\sqrt{\Delta} & \text{if}\quad \Delta_1<0,\ \Delta_2<0\,,\\ \sqrt{\Delta} & \text{otherwise}\,.\end{cases}$$

Proof of **A.** The factorization of Δ can be deduced from Exercise 1.1.7, but it can also be seen by an elementary argument as follows.

We set $\Delta=2^eD$, where $e\in\{0,2,3\}$ and $D\in\mathbb{Z}\setminus2\mathbb{Z}$. If $e=3$, then $|D|\ne1$, and if $\varepsilon\in\{\pm1\}$ is such that $D\equiv\varepsilon \mod 4$, then $\Delta=(8\varepsilon)(\varepsilon D)$ is the desired factorization. If $e=2$, then again $|D|\ne1$, $D\equiv 3 \mod 4$, and $\Delta=(-4)(-D)$ is the desired factorization. If $e=0$, then $D\equiv1\mod 4$, $D=D_1D_2$, where D_1, $D_2\in\mathbb{Z}$ are squarefree, $|D_1|>1$, $|D_2|>1$, $(D_1,D_2)=1$, and $D_1\equiv D_2 \mod 4$. If $\varepsilon\in\{\pm1\}$ and $D_1\equiv D_2\equiv\varepsilon \mod 4$, then $D=(\varepsilon D_1)(\varepsilon D_2)$ is the desired factorization.

Let now $\Delta=\Delta_1\Delta_2$ be a factorization of Δ into fundamental discriminants Δ_1, Δ_2 such that $(\Delta_1,\Delta_2)=1$. By Theorem A.3.5.2, there is a bijective map

$$\Phi\colon(\mathbb{Z}/|\Delta_1|\mathbb{Z})^\times\times(\mathbb{Z}/|\Delta_2|\mathbb{Z})^\times\to(\mathbb{Z}/|\Delta|\mathbb{Z})^\times$$

such that

$$\Phi(t_1'+|\Delta_1|\mathbb{Z},t_2'+|\Delta_2|\mathbb{Z})=t_1'|\Delta_2|+t_2'|\Delta_1|+|\Delta|\mathbb{Z}$$

for all $(t_1',t_2')\in\mathbb{Z}^2$ satisfying $(t_i',\Delta_i)=1$ for $i\in\{1,2\}$.

For $i\in\{1,2\}$ and $t_i\in\mathbb{Z}/|\Delta_i|\mathbb{Z}$, we fix some representative $t_i'\in\mathbb{N}$ satisfying $t_i=t_i'+|\Delta_i|\mathbb{Z}$. Then we obtain

$$\begin{aligned}\tau(\mathsf{Q}_\Delta)&=\sum_{t\in(\mathbb{Z}/|\Delta|\mathbb{Z})^\times}\mathsf{Q}_\Delta(t)\zeta_{|\Delta|}^t\\&=\sum_{t_1\in(\mathbb{Z}/|\Delta_1|\mathbb{Z})^\times}\ \sum_{t_2\in(\mathbb{Z}/|\Delta_2|\mathbb{Z})^\times}\mathsf{Q}_\Delta(t_1'|\Delta_2|+t_2'|\Delta_1|)\zeta_{|\Delta|}^{t_1'|\Delta_2|+t_2'|\Delta_1|}\,.\end{aligned}$$

Throughout the following calculations, we use the Theorems 3.5.1 and 3.5.4. First we fix some $(t_1,t_2) \in (\mathbb{Z}/|\Delta_1|\mathbb{Z})^\times \times (\mathbb{Z}/|\Delta_2|\mathbb{Z})^\times$. Then $\zeta_{|\Delta|}^{t_1'|\Delta_2|+t_2'|\Delta_1|} = \zeta_{|\Delta_1|}^{t_1}\zeta_{|\Delta_2|}^{t_2}$, and

$$\begin{aligned}
\mathsf{Q}_\Delta(t_1'|\Delta_2|+t_2'|\Delta_1|) &= \Big(\frac{\Delta}{t_1'|\Delta_2|+t_2'|\Delta_1|}\Big) = \Big(\frac{\Delta_1}{t_1'|\Delta_2|+t_2'|\Delta_1|}\Big)\Big(\frac{\Delta_2}{t_1'|\Delta_2|+t_2'|\Delta_1|}\Big) \\
&= \Big(\frac{\Delta_1}{t_1'|\Delta_2|}\Big)\Big(\frac{\Delta_2}{t_2'|\Delta_1|}\Big) = \Big(\frac{\Delta_1}{|\Delta_2|}\Big)\Big(\frac{\Delta_2}{|\Delta_1|}\Big)\Big(\frac{\Delta_1}{t_1'}\Big)\Big(\frac{\Delta_2}{t_2'}\Big) \\
&= \sigma(\Delta_1,\Delta_2)\mathsf{Q}_{\Delta_1}(t_1)\mathsf{Q}_{\Delta_2}(t_2)\,,
\end{aligned}$$

where

$$\sigma(\Delta_1,\Delta_2) = \begin{cases} -1 & \text{if} \quad \Delta_1 < 0 \text{ and } \Delta_2 < 0\,, \\ 1 & \text{otherwise.} \end{cases}$$

For the proof of the last equality, observe that $\Delta_1 \equiv 1 \bmod 4$ or $\Delta_2 \equiv 1 \bmod 4$, and therefore

$$\Big(\frac{\Delta_1}{|\Delta_2|}\Big)\Big(\frac{\Delta_2}{|\Delta_1|}\Big) = \Big(\frac{\Delta_1}{\operatorname{sgn}(\Delta_2)}\Big)\Big(\frac{\Delta_2}{\operatorname{sgn}(\Delta_1)}\Big)\Big(\frac{\Delta_1}{\Delta_2}\Big)\Big(\frac{\Delta_2}{\Delta_1}\Big) = \sigma(\Delta_1,\Delta_2)^3 = \sigma(\Delta_1,\Delta_2)\,.$$

Hence we obtain

$$\begin{aligned}
\tau(\mathsf{Q}_\Delta) &= \sigma(\Delta_1,\Delta_2)\sum_{t_1\in(\mathbb{Z}/|\Delta_1|\mathbb{Z})^\times}\ \sum_{t_2\in(\mathbb{Z}/|\Delta_2|\mathbb{Z})^\times} \mathsf{Q}_{\Delta_1}(t_1)\mathsf{Q}_{\Delta_2}(t_2)\zeta_{|\Delta_1|}^{t_1}\zeta_{|\Delta_2|}^{t_2} \\
&= \sigma(\Delta_1,\Delta_2)\tau(\mathsf{Q}_{\Delta_1})\tau(\mathsf{Q}_{\Delta_2})\,.
\end{aligned}$$

□

Exercise 3.5.9. For $k \in \mathbb{N}$ and $m \in \mathbb{Z}$, we define

$$g(m,k) = \sum_{n=0}^{k-1} \zeta_k^{mn^2}\,.$$

Prove the following assertions.

a) If $t \in \mathbb{Z}$, $a,\ b \in \mathbb{N}$ and $(a,b)=1$, then $g(tb,a)g(ta,b) = g(t,ab)$.

b) If p is an odd prime, φ_p is the quadratic character modulo p and $m \in \mathbb{Z}\setminus p\mathbb{Z}$, then

$$g(m,p) = \Big(\frac{m}{p}\Big)\tau(\varphi_p)\,.$$

c) If p, q are distinct odd primes, then $g(1,pq) = \sqrt{(-1)^{(pq-1)/2}pq}$.

We continue with an explicit description of all real characters for an arbitrary modulus. On this occasion we shall also determine the primitives among them and obtain a counterpart to Theorem 3.5.6.

Theorem 3.5.10. *Suppose that* $m = 2^e p_1^{e_1}\cdot\ldots\cdot p_r^{e_r} \ge 2$, *where* $r,\ e \in \mathbb{N}_0$, $p_1,\ldots,p_r$ *are distinct odd primes and* $e_1,\ldots,e_r \in \mathbb{N}$. *Note that for* $a \in \mathbb{Z}$ *the residue classes* $a+p_1\mathbb{Z},\ldots,a+p_r\mathbb{Z}$ *and* $a+2^e\mathbb{Z}$ *are uniquely determined by the residue class* $a+m\mathbb{Z}$. *We set*

$$\rho = \begin{cases} r & \textit{if} \quad e \le 1\,, \\ r+1 & \textit{if} \quad e = 2\,, \\ r+2 & \textit{if} \quad e = 3\,, \end{cases}$$

and we define quadratic characters $\varphi_1,\ldots,\varphi_\rho\colon (\mathbb{Z}/m\mathbb{Z})^\times \to \{\pm 1\}$ *as follows*:

For $a\in\mathbb{Z}$ *such that* $(a,m)=1$, *we set*

$$\varphi_i(a+m\mathbb{Z}) = \Big(\frac{a}{p_i}\Big) \quad \textit{for}\;\; i\in[1,r]\,.$$

$$\varphi_{r+1}(a+m\mathbb{Z}) = \Big(\frac{-1}{a}\Big) = (-1)^{(a-1)/2} \quad \textit{if}\;\; e\ge 2\,,$$

and

$$\varphi_{r+2}(a+m\mathbb{Z}) = \Big(\frac{2}{a}\Big) = (-1)^{(a^2-1)/8} \quad \textit{if}\;\; e\ge 3\,.$$

1. $(\varphi_1,\ldots,\varphi_\rho)$ *is a basis of the elementary* 2*-group* $\mathsf{X}(m)[2]$ *of all real characters modulo* m, *and*

$$|\mathsf{X}(m)[2]| = \big((\mathbb{Z}/m\mathbb{Z})^\times : (\mathbb{Z}/m\mathbb{Z})^{\times 2}\big) = 2^\rho\,.$$

2. *For a real character* $\varphi\in\mathsf{X}(m)$, *the following assertions are equivalent*:
   - (a) φ *is primitive.*
   - (b) $e\in\{0,2,3\}$, $e_i=1$ *for all* $i\in[1,r]$, *and either* $\varphi=\varphi_1\cdot\ldots\cdot\varphi_\rho$, *or* $e=3$ *and* $\varphi=\varphi_1\cdot\ldots\cdot\varphi_r\varphi_{r+2}$.
   - (c) $\Delta=\varphi(-1)m$ *is a fundamental discriminant, and* $\varphi=\mathsf{Q}_\Delta$.

PROOF. For $i\in[1,r]$, let $\pi_i\in\mathbb{Z}$ be such that

$$\langle \pi_i + p_i^{e_i}\mathbb{Z}\rangle = (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times \quad\text{and}\quad \pi_i\equiv 1 \bmod \frac{m}{p_i^{e_i}}\,.$$

If $e\ge 2$, let $\pi_{r+1}\in\mathbb{Z}$ be such that

$$\pi_{r+1}\equiv -1 \bmod 2^e \quad\text{and}\quad \pi_{r+1}\equiv 1 \bmod \frac{m}{2^e}\,.$$

If $e\ge 3$, let $\pi_{r+2}\in\mathbb{Z}$ be such that

$$\pi_{r+2}\equiv 5 \bmod 2^e \quad\text{and}\quad \pi_{r+2}\equiv 1 \bmod \frac{m}{2^e}\,.$$

Then $(\pi_1+m\mathbb{Z},\ldots,\pi_\rho+m\mathbb{Z})$ is a basis of $(\mathbb{Z}/m\mathbb{Z})^\times$ (see Theorem A.6.5), and obviously $2\,|\,\mathrm{ord}(\pi_i+m\mathbb{Z})$ for all $i\in[1,\rho]$.

1. It suffices to prove the following assertion:

A. For all i, $j\in[1,\rho]$, we have

$$(*)\qquad \varphi_i(\pi_j+m\mathbb{Z}) = \begin{cases} -1 & \text{if}\;\; i=j\,,\\ 1 & \text{if}\;\; i\ne j\,.\end{cases}$$

Indeed, suppose that **A** holds. If i, $j\in[1,\rho]$ and $i\ne j$, then $\varphi_i\,|\,\langle\pi_i+m\mathbb{Z}\rangle$ is the unique quadratic character of the cyclic subgroup $\langle\pi_i+m\mathbb{Z}\rangle$ of $(\mathbb{Z}/m\mathbb{Z})^\times$, and $\varphi_i\,|\,\langle\pi_j+m\mathbb{Z}\rangle=\mathbf{1}_m$. Hence $(\varphi_1,\ldots,\varphi_\rho)$ is a basis of $\mathsf{X}(m)[2]$ by Corollary A.7.4, and $|\mathsf{X}(m)| = ((\mathbb{Z}/m\mathbb{Z})^\times : (\mathbb{Z}/m\mathbb{Z})^{\times 2}) = 2^\rho$.

Proof of **A.** Suppose that $i \in [1,r]$. Then $\pi_i + p_i^{e_i}\mathbb{Z}$ is not a square in $(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times$, hence π_i is not a quadratic residue modulo $p_i^{e_i}$ and thus it is not a quadratic residue modulo p_i by Theorem 3.1.5.1. Hence

$$\varphi_i(\pi_i + m\mathbb{Z}) = \Big(\frac{\pi_i}{p_i}\Big) = -1\,.$$

If $j \in [1,r] \setminus \{i\}$, then $\pi_i \equiv 1 \bmod p_j$, and therefore

$$\varphi_j(\pi_i + m\mathbb{Z}) = \Big(\frac{\pi_i}{p_j}\Big) = 1\,.$$

If $e \ge 2$, then $\pi_i \equiv 1 \bmod 2^e$, and therefore $\varphi_j(\pi_i + m\mathbb{Z}) = 1$ for $j \in [r+1,\rho]$.

If $e \ge 2$, then $\pi_{r+1} \equiv -1 \bmod 2^e$ and $\pi_{r+1} \equiv 1 \bmod p_j$ for all $j \in [1,r]$. Hence $\varphi_{r+1}(\pi_{r+1} + m\mathbb{Z}) = -1$, $\varphi_j(\pi_{r+1} + m\mathbb{Z}) = 1$ for all $j \in [1,r]$, and, if $e \ge 3$, then $\varphi_{r+2}(\pi_{r+1} + m\mathbb{Z}) = 1$.

If $e \ge 3$, then $\pi_{r+2} \equiv 5 \bmod 2^e$ and $\pi_{r+2} \equiv 1 \bmod p_j$ for all $j \in [1,r]$. Hence $\varphi_{r+2}(\pi_{r+2} + m\mathbb{Z}) = -1$ and $\varphi_j(\pi_{r+2} + m\mathbb{Z}) = 1$ for all $i \in [1, r+1]$.

2. We set $P = p_1 \cdot \ldots \cdot p_r$.

(a) $\Rightarrow$ (b) Let $\varphi \in \mathsf{X}(m)$ be a primitive real character. Then there exists a subset $I \subset [1,\rho]$ such that

$$\varphi = \prod_{i\in I} \varphi_i\,, \quad \text{and we set } m' = 2^{e'}P, \text{ where } \ e' = \begin{cases} 0 & \text{if } \ e \le 1\,, \\ 2 & \text{if } \ e = 2\,, \\ 3 & \text{if } \ e \ge 3\,. \end{cases}$$

If $a \in \mathbb{Z}$, $(a,m) = 1$ and $a \equiv 1 \bmod m'$, then $\varphi_i(a) = 1$ for all $i \in [1,\rho]$, hence $\varphi(a) = 1$, and therefore $m' = m$. It remains to prove that either $I = [1,\rho]$, or $e = 3$ and $I = [1,r] \cup \{r+2\}$. We assume the contrary and prove that there exists a proper positive divisor k of m such that $\varphi(a) = 1$ for all $a \in \mathbb{Z}$ such that $(a,m) = 1$ and $a \equiv 1 \bmod k$. Indeed,

- if $i \in [1,r] \setminus I$, then we obtain $\varphi(a) = 1$ for all $a \in \mathbb{Z}$ satisfying $(a,m) = 1$ and $a \equiv 1 \bmod mp_i^{-1}$;
- if $e = 2$ and $r+1 \notin I$, then we obtain $\varphi(a) = 1$ for all $a \in \mathbb{Z}$ satisfying $(a,m) = 1$ and $a \equiv 1 \bmod P$;
- if $e = 3$ and $r+2 \notin I$, then we obtain $\varphi(a) = 1$ for all $a \in \mathbb{Z}$ satisfying $(a,m) = 1$ and $a \equiv 1 \bmod 4P$.

(b) $\Rightarrow$ (c) We set $\phi = \varphi_1 \cdot \ldots \cdot \varphi_r$. If $a \in \mathbb{Z}$ and $(a,m) = 1$, then

$$\begin{aligned} \phi(a) &= \prod_{i=1}^r \Big(\frac{a}{p_i}\Big) = \Big(\frac{a}{P}\Big) \\ &= \Big(\frac{P}{a}\Big)(-1)^{\frac{P-1}{2}\frac{a-1}{2}} = \Big(\frac{P}{a}\Big)\Big(\frac{-1}{a}\Big)^{(P-1)/2} = \Big(\frac{(-1)^{(P-1)/2}P}{a}\Big)\,. \end{aligned}$$

CASE 1: $e = 0$. Then $m = P$, $\varphi = \phi$, and $\Delta = \varphi(-1)m = (-1)^{(m-1)/2}m$ is a fundamental discriminant. If $a \in \mathbb{Z}$ and $(a,m) = 1$, then

$$\mathsf{Q}_\Delta(a) = \Big(\frac{a}{m}\Big) = \varphi(a)\,.$$

CASE 2: $e=2$. Then $m=4P$, $\varphi=\phi\varphi_{r+1}$,

$$\varphi(-1)=\phi(-1)\varphi_{r+1}(-1)=-(-1)^{(P-1)/2}=\begin{cases}1 & \text{if } \ P\equiv 3 \mod 4\,,\\ -1 & \text{if } \ P\equiv 1 \mod 4\,,\end{cases}$$

and therefore $\Delta=4\varphi(-1)P$ is a fundamental discriminant. If $a\in\mathbb{Z}$ and $(a,m)=1$, then

$$\mathsf{Q}_\Delta(a)=\Big(\frac{\Delta}{a}\Big)=\Big(\frac{\varphi(-1)P}{a}\Big)=\Big(\frac{-1}{a}\Big)\Big(\frac{(-1)^{(P-1)/2}P}{a}\Big)=(\varphi_{r+1}\phi)(a)=\varphi(a)\,.$$

CASE 3: $e=3$. Then $m=8P$, $\varphi=\phi\varphi_{r+2}$ or $\varphi=\phi\varphi_{r+1}\varphi_{r+2}$. In any case, $\Delta=8\,\varphi(-1)P$ is a fundamental discriminant. Let $a\in\mathbb{Z}$ be such that $(a,m)=1$.

If $\varphi=\phi\varphi_{r+2}$, then $\varphi(-1)=\phi(-1)=(-1)^{(P-1)/2}$, and

$$\begin{aligned}\mathsf{Q}_\Delta(a)&=\Big(\frac{\Delta}{a}\Big)=\Big(\frac{8(-1)^{(P-1)/2}P}{a}\Big)=\Big(\frac{2}{a}\Big)\Big(\frac{(-1)^{(P-1)/2}P}{a}\Big)\\&=(\varphi_{r+2}\phi)(a)=\varphi(a)\,.\end{aligned}$$

If $\varphi=\phi\varphi_{r+1}\varphi_{r+2}$. Then $\varphi(-1)=-\phi(-1)=-(-1)^{((P-1)/2}$, and

$$\begin{aligned}\mathsf{Q}_\Delta(a)&=\Big(\frac{\Delta}{a}\Big)=\Big(\frac{-8(-1)^{(P-1)/2}P}{a}\Big)=\Big(\frac{-1}{a}\Big)\Big(\frac{2}{a}\Big)\Big(\frac{(-1)^{(P-1)/2}P}{a}\Big)\\&=(\varphi_{r+1}\varphi_{r+2}\phi)(a)=\varphi(a)\,.\end{aligned}$$

(c) $\Rightarrow$ (a) By Theorem 3.5.6. □

We conclude this section with a new formula for the number of solutions of a quadratic congruence using Kronecker symbols (Theorem 3.5.11). This formula will be used in Chapter 6 to obtain quantitative results concerning the representation of integers by binary quadratic forms (see Theorem 6.2.12).

Theorem 3.5.11. *Let $m\in\mathbb{N}$ and $a\in\mathbb{Z}$ be integers such that $(a,m)=1$, $a\equiv 0$ or $1 \bmod 4$, and*

$$N_m(a)=|\{x+4m\mathbb{Z}\in\mathbb{Z}/4m\mathbb{Z}\mid x^2\equiv a \mod 4m\,\}|\,.$$

1. *If m_0 is the square-free kernel of m, then*

$$N_m(a)=2\sum_{1\le d\,|\,m_0}\Big(\frac{a}{d}\Big)\,,$$

2. *a is a quadratic residue modulo $4m$ if and only if*

$$\Big(\frac{a}{p}\Big)=1 \quad \textit{for all primes } p \textit{ dividing } m, \textit{ and then } \ N_m(a)=2^{r+1}\,,$$

where r is the number of distinct primes dividing m.

Proof. Suppose that $m=2^e p_1^{e_1}\cdot\ldots\cdot p_s^{e_s}$, where $e,\,s\in\mathbb{N}_0$, $p_1,\ldots,p_s$ are distinct odd primes, and $e_1,\ldots,e_s\in\mathbb{N}$. By the Chinese remainder theorem, we obtain

$$N_m(a)=|\{x+4m\mathbb{Z}\in\mathbb{Z}/4m\mathbb{Z}\mid x^2\equiv a \mod 4m\,\}|=\prod_{i=0}^{s}N_i\,,$$

where

$$N_0 = |\{x + 2^{e+2}\mathbb{Z} \in \mathbb{Z}/2^{e+2}\mathbb{Z} \mid x^2 \equiv a \mod 2^{e+2}\}| = \begin{cases} 2 & \text{if} \quad e = 0\,, \\ 2\big[1 + \big(\frac{a}{2}\big)\big] & \text{if} \quad e \ge 1\,, \end{cases}$$

$$N_i = |\{x + p_i^{e_i}\mathbb{Z} \in \mathbb{Z}/2^{e_i}\mathbb{Z} \mid x^2 \equiv a \mod p_i^{e_i}\}| = 1 + \Big(\frac{a}{p_i}\Big) \quad \text{for all } \ i \in [1, s],$$

and therefore

$$N_m(a) = \prod_{i=0}^{s} N_i = 2 \prod_{\substack{p \in \mathbb{P} \\ p \,|\, m_0}} \Big[1 + \Big(\frac{a}{p}\Big)\Big] = 2 \sum_{1 \le d \,|\, m_0} \Big(\frac{a}{d}\Big)\,.$$

By Theorem 3.1.2, a is a quadratic residue modulo $4m$ if and only if a is a quadratic residue modulo 2^{e+2} and modulo $p_i^{e_i}$ for all $i \in [1, s]$. Now we apply Theorem 3.1.5. If $e = 0$, then a is a quadratic residue modulo 4 by assumption. If $e \ge 1$, then $(a, m) = 1$ implies $a \equiv 1 \bmod 4$, and a is a quadratic residue modulo 2^{e+2} if and only if $a \equiv 1 \mod 8$, that is, if and only if $\big(\frac{a}{2}\big) = 1$. For all $i \in [1, s]$, a is a quadratic residue modulo $p_i^{e_i}$ if and only if a is a quadratic residue modulo p_i. Hence it follows that a is a quadratic residue modulo $4m$ if and only if $\big(\frac{a}{p}\big) = 1$ for all primes p dividing m.

In the calculations made above, we set

$$N_0 = 4 \ \text{ if } \ e \ge 1\,, \qquad r = \begin{cases} s & \text{if} \quad 2 \nmid m\,, \\ s + 1 & \text{if} \quad 2 \,|\, m\,, \end{cases}$$

and then it follows that $N_m(a) = 2^{r+1}$. □

This page intentionally left blank

CHAPTER 4

L-series and Dirichlet's prime number theorem

4.1. Preliminaries and some elementary cases

The main purpose of this chapter is a proof of the following Theorem 4.1.1, called Dirichlet's theorem on primes in arithmetic progressions or Dirichlet's prime number theorem.

Theorem 4.1.1 (Dirichlet's prime number theorem)**.** *Let m and k be positive integers. If $(m,k)=1$, then the arithmetic progression $k+m\mathbb{N}$ contains infinitely many primes* [*equivalently, there are infinitely many primes $p \equiv k \bmod m$*].

The full proof of Dirichlet's prime number theorem needs analytic methods. There exist proofs avoiding the analytic machinery, but they are not really elementary and are beyond the scope of our book (see, e.g., [**96**]). The idea for the analytic proof is to consider the convergent (eventually infinite) series

$$\sum_{\substack{p\in\mathbb{P}\\ p\,\equiv\, k \bmod m}} \frac{1}{p^s} \quad \text{for } s \in \mathbb{R}_{>1}$$

and to prove that it tends to infinity as $s \to 1$. For this proof, we develop the basics of the theory of multiplicative functions and Dirichlet's L-series in the Sections 4.2 and 4.3. These results will be used again in Chapter 8 when we investigate the analytic theory of quadratic orders and binary quadratic forms. The actual proof of Dirichlet's prime number theorem will be completed at the end of Section 4.3. In Section 4.4, we deal with the summation of L-series and pave the way for the proof of the analytic class number formula in Chapter 8.

For a deeper study of analytic number theory, a thorough knowledge of complex analysis is indispensable. To get an impression, the reader may consult the textbooks [**45**], [**12**], or (more elementary) [**2**]. A concise axiomatic approach can be found in [**33**]. In the present volume, our requirements are more modest. Besides standard real analysis of one variable, we shall use only basics from the theory of complex variables. In Appendix B the reader may find those analytic prerequisites which usually are not covered in an introductory course.

Exercise 4.1.2. Let $a \in \mathbb{Z}$ be not a square. Use Dirichlet's prime number theorem to prove that there exist infinitely many primes p such that a is a quadratic residue modulo p and also infinitely many primes such that a is a quadratic non-residue modulo p.

We proceed with the discussion of some special cases of Dirichlet's prime number theorem which can be handled by elementary methods without analytic tools. We deal with the unit class in Theorem 4.1.4, with the prime residue classes modulo 8 in Theorem 4.1.5, and leave the prime residue classes modulo 12 as an exercise. We start with a simple observation.

Theorem 4.1.3. *Let m and k be coprime positive integers, and suppose that for every $l \in \mathbb{N}$ there is some prime $p \ne k$ satisfying $p \equiv k \bmod m^l$. Then there are infinitely many primes $p \equiv k \bmod m$.*

PROOF. Assume to the contrary that there are only finitely many primes p such that $p \equiv k \bmod m$, say $\{p \in \mathbb{P} \mid p \ne k\,,\ p \equiv k \bmod m\} = \{p_1, \ldots, p_r\}$, where $r \in \mathbb{N}$ and $p_1, \ldots, p_r$ are distinct. Let $l \in \mathbb{N}$ be such that $m^l \nmid (p_1 - k) \cdot \ldots \cdot (p_r - k)$. By assumption, there exists some prime $p \ne k$ such that $p \equiv k \bmod m^l$, and thus $p \notin \{p_1, \ldots, p_r\}$, a contradiction. □

The following proof of Dirichlet's prime number theorem for the unit class is taken from [**95**].

Theorem 4.1.4. *For every positive integer $m \ge 2$ there exist infinitely many primes $p \equiv 1 \bmod m$.*

PROOF. We make use of two auxiliary results.

I. If $n \in \mathbb{N}$ and $x_1, \ldots, x_n \in \mathbb{R}$, then

$$\max\{x_1, \ldots, x_n\} = \sum_{\emptyset \ne I \subset [1,n]} (-1)^{|I|-1} \min\{x_i \mid i \in I\}\,.$$

II. If $a,\ m \in \mathbb{N}_{\ge 2},\ \ n \in \mathbb{N}$ and $p_1, \ldots, p_n$ are distinct primes dividing m, then

$$(a^{m/p_1} - 1, \ldots, a^{m/p_n} - 1) = a^{m/p_1 \cdot \ldots \cdot p_n} - 1\,.$$

Proof of **I.** As both sides of the asserted equation are symmetric in $x_1, \ldots, x_n$, we may assume that $x_1 \le x_2 \le \ldots \le x_n$, and then we obtain

$$\begin{aligned}
&\sum_{\emptyset \ne I \subset [1,n]} (-1)^{|I|-1} \min\{x_i \mid i \in I\} \\
&= \sum_{\emptyset \ne I \subset [1,n-1]} (-1)^{|I|-1} \min\{x_i \mid i \in I\} + \sum_{I \subset [1,n-1]} (-1)^{|I|} \min\{x_i \mid i \in I \cup \{n\}\} \\
&= \sum_{\emptyset \ne I \subset [1,n-1]} (-1)^{|I|-1} \min\{x_i \mid i \in I\} + \sum_{\emptyset \ne I \subset [1,n-1]} (-1)^{|I|} \min\{x_i \mid i \in I\} + x_n = x_n\,.
\end{aligned}$$

Proof of **II.** It is well known (see Theorem A.3.1) that

$$(a^{m/p_1} - 1, \ldots, a^{m/p_n} - 1) = a^d - 1\,, \quad \text{where} \quad d = \Big(\frac{m}{p_1}, \ldots, \frac{m}{p_n}\Big)\,.$$

Since $p_1 \cdot \ldots \cdot p_n d = m \gcd(\{p_1 \cdot \ldots \cdot p_{i-1} p_{i+1} \cdot \ldots \cdot p_n \mid i \in [1,n]\}) = m$, it follows that

$$d = \frac{m}{p_1 \cdot \ldots \cdot p_n}\,.$$

Now we can prove the theorem. By Theorem 4.1.3 it suffices to prove that for every $m \ge 2$ there exists some prime $p \equiv 1 \bmod m$. Suppose that $m \ge 2$, and let $p_1, \ldots, p_r$ be the distinct prime factors of m. We consider the number

$$N = \frac{m^m - 1}{\operatorname{lcm}\{m^{m/p_1} - 1, \ldots m^{m/p_r} - 1\}}\,.$$

Since $m^{m/p_i} - 1 \,|\, m^m - 1$ for all $i \in [1, r]$, it follows that $N \in \mathbb{N}$, and we assert that $N > 1$. Assume to the contrary that $m^m - 1 = \operatorname{lcm}\{m^{m/p_1} - 1, \ldots m^{m/p_r} - 1\}$. For every prime p, **I.** implies

$$\begin{aligned}\mathsf{v}_p(m^m - 1) &= \max\{\mathsf{v}_p(m^{m/p_i} - 1) \mid i \in [1, r]\} \\ &= \sum_{\emptyset \ne I \subset [1,r]} (-1)^{|I|-1} \min\{\mathsf{v}_p(m^{m/p_i} - 1) \mid i \in I\}\,,\end{aligned}$$

and, for every $\emptyset \ne I \subset [1, r]$, **II.** implies

$$\begin{aligned}\min\{\mathsf{v}_p(m^{m/p_i} - 1) \mid i \in I\} &= \mathsf{v}_p\big(\gcd\{m^{m/p_i} - 1 \mid i \in I\}\big) \\ &= \mathsf{v}_p(m^{m/p_I} - 1)\,, \quad \text{where} \quad p_I = \prod_{i \in I} p_i\,.\end{aligned}$$

Consequently

$$0 = \sum_{I \subset [1,r]} (-1)^{|I|} \mathsf{v}_p(m^{m/p_I} - 1) = \mathsf{v}_p\Big(\prod_{I \subset [1,r]} (m^{m/p_I} - 1)^{(-1)^{|I|}}\Big)\,,$$

and since this holds for all primes p, we obtain

$$\prod_{I \subset [1,r]} (m^{m/p_I} - 1)^{(-1)^{|I|}} = 1\,,$$

and therefore

$$\prod_{\substack{I \subset [1,r] \\ |I| \equiv 0 \bmod 2}} (m^{m/p_I} - 1) \;-\; \prod_{\substack{I \subset [1,r] \\ |I| \equiv 1 \bmod 2}} (m^{m/p_I} - 1) = 0\,.$$

If $I \subsetneq [1, r]$, then $m^{m/p_I} \equiv 0 \bmod m^{m/p_1 \cdot \ldots \cdot p_r + 1}$, and thus it follows that

$$\pm(m^{p_1 \cdot \ldots \cdot p_r} - 1) = \prod_{\substack{I \subsetneq [1,r] \\ |I| \equiv 0 \bmod 2}} (m^{m/p_I} - 1) \;-\; \prod_{\substack{I \subsetneq [1,r] \\ |I| \equiv 1 \bmod 2}} (m^{m/p_I} - 1) \equiv 0 \bmod m^{m/p_1 \cdot \ldots \cdot p_r + 1}\,,$$

a contradiction.

Let p be a prime divisor of N. Then $m^m \equiv 1 \bmod p$, and we assert that m is the order of $m + p\mathbb{Z} \in (\mathbb{Z}/p\mathbb{Z})^\times$. Once this is proved, then it follows that $m \,|\, p - 1$ and thus $p \equiv 1 \bmod m$.

Assume to the contrary that $m^{m/p_i} \equiv 1 \bmod p$ for some $i \in [1, r]$. Then

$$\frac{m^m - 1}{m^{m/p_i} - 1} = \sum_{k=0}^{p_i - 1} (m^{m/p_i})^k \equiv p_i \bmod p \quad \text{and} \quad p \,|\, N \,\Big|\, \frac{m^m - 1}{m^{m/p_i} - 1}\,,$$

a contradiction, since $p \ne p_i$. □

Theorem 4.1.5. *For each* $k \in \{3,5,7\}$, *there exist infinitely many primes* p *such that* $p \equiv k \bmod 8$.

Proof. The proof is modeled upon Euclid's proof of the infinitude of primes. We suppose that, for some $r \in \mathbb{N}$, there exist already primes $p_1, \ldots p_r$ congruent to k modulo 8, and then we construct yet another such prime. We set $N = p_1 \cdot \ldots \cdot p_r$, and we apply the Theorems 3.3.1 and 3.3.5.

$k = 3$: If $a = N^2 + 2$ and p is any prime dividing a, then -2 is a quadratic residue modulo p and therefore $p \equiv 1$ or $3 \bmod 8$. Since $a \equiv 3 \bmod 8$, there exists a prime divisor p of a such that $p \equiv 3 \bmod 8$, and clearly $p \notin \{p_1, \ldots, p_r\}$.

$k = 5$: If $a = N^2 + 4$ and p is a prime divisor of a, then $N^2 \equiv -4 \bmod p$, hence

$$\Big(\frac{-4}{p}\Big) = \Big(\frac{-1}{p}\Big) = 1\,, \quad \text{and thus} \quad p \equiv 1 \mod 4\,.$$

Since $a \equiv 5 \bmod 8$, there exists a prime divisor p of a such that $p \equiv 5 \bmod 8$, and clearly $p \notin \{p_1, \ldots, p_r\}$.

$k = 7$: If $a = N^2 - 2$ and p is a prime dividing a, then 2 is a quadratic residue modulo p and thus $p \equiv 1$ or $7 \bmod 8$. Since $a \equiv 7 \bmod 8$, there exists a prime divisor p of a such that $p \equiv 7 \bmod 8$, and clearly $p \notin \{p_1, \ldots, p_r\}$. □

Exercise 4.1.6. Suppose that $k \in \{5,7,11\}$, and prove that there exist infinitely many primes $p \equiv k \bmod 12$. (Compare [**97**].)

4.2. Multiplicative functions

Definition 4.2.1. A function $f\colon \mathbb{N} \to \mathbb{C}$ is called

- *multiplicative* if $f(m_1m_2) = f(m_1)f(m_2)$ for all m_1, $m_2 \in \mathbb{N}$ such that $(m_1, m_2) = 1$;
- *completely multiplicative* if $f(m_1m_2) = f(m_1)f(m_2)$ for all m_1, $m_2 \in \mathbb{N}$.

If $f \neq 0$ is a multiplicative function, then $f(1) = 1$, and

$$f(n) = \prod_{p \in \mathbb{P}} f(p^{\mathsf{v}_p(n)}) \quad \text{for all } n \in \mathbb{N}.$$

In particular, a multiplicative function $f \neq 0$ is uniquely determined by its values on prime powers.

Euler's φ function $\varphi\colon \mathbb{N} \to \mathbb{N} \hookrightarrow \mathbb{C}$ (see Definition A.6.2) is multiplicative. The point-wise product of two (completely) multiplicative functions is (completely) multiplicative. For every $s \in \mathbb{R}$, the function $n \mapsto n^s$ is completely multiplicative. If $m \in \mathbb{N}$, then every Dirichlet character $\chi \in \mathsf{X}(m)$ is a completely multiplicative function $\chi\colon \mathbb{N} \to \mathbb{C}$. In particular, if $\chi \in \mathsf{X}(m)$ and $s \in \mathbb{R}$, then the function $n \mapsto \chi(n)n^s$ is completely multiplicative.

Theorem 4.2.2. *Let* $f\colon \mathbb{N}\to\mathbb{C}$ *be a multiplicative function. Then its summatory function*

$$\mathsf{S}f\colon \mathbb{N}\to\mathbb{C}\,, \quad \textit{defined by} \quad (\mathsf{S}f)(n)=\sum_{d\,|\,n} f(d)\,, \quad \textit{is also multiplicative.}$$

Proof. Let $m_1,\ m_2\in\mathbb{N}$ be such that $(m_1,m_2)=1$. If $d\in\mathbb{N}$, then $d\,|\,m_1m_2$ if and only if there exist $d_1,\ d_2\in\mathbb{N}$ such that $d_1\,|\,m_1,\ \ d_2\,|\,m_2$ and $d=d_1d_2$. Hence

$$\begin{aligned}(\mathsf{S}f)(m_1m_2) &= \sum_{d\,|\,m_1m_2} f(d)=\sum_{d_1|\,m_1}\sum_{d_2|\,m_2} f(d_1d_2)\\ &= \sum_{d_1|\,m_1}\sum_{d_2|\,m_2} f(d_1)f(d_2)=(\mathsf{S}f)(m_1)(\mathsf{S}f)(m_2)\,. \qquad \square\end{aligned}$$

Multiplicative functions are a powerful tool in number theory. Some of their interesting properties (which however will not be used in this volume) are collected in the following exercise.

Exercise 4.2.3. For two functions $f,\ g\colon\mathbb{N}\to\mathbb{C}$, we define their *Dirichlet convolution* $f*g\colon\mathbb{N}\to\mathbb{C}$ by

$$f*g(n)=\sum_{d\,|\,n} f(d)g\Big(\frac{n}{d}\Big)\,.$$

The *Möbius function* $\mu\colon\mathbb{N}\to\{0,\pm1\}\subset\mathbb{C}$ is the unique multiplicative function such that, for all primes p and $e\in\mathbb{N}$,

$$\mu(p^e)=\begin{cases}-1 & \text{if} \quad e=1\,,\\ 0 & \text{if} \quad e>1\,.\end{cases}$$

The completely multiplicative functions $\varepsilon,\ \iota\colon\mathbb{N}\to\mathbb{C}$ are defined by

$$\varepsilon(n)=\begin{cases}1 & \text{if} \quad n=1\,,\\ 0 & \text{if} \quad n>1\,,\end{cases} \qquad \text{and} \quad \iota(n)=1 \ \text{ for all } \ n\in\mathbb{N}\,.$$

Prove the following assertions:

a) The composition $*$ is commutative and associative, and $f*\varepsilon=f$ for every function $f\colon\mathbb{N}\to\mathbb{C}$.

b) If $f,\ g\colon\mathbb{N}\to\mathbb{C}$ are multiplicative functions, then $f*g$ is also multiplicative. The relation $\mathsf{S}f=f*\iota$ yields a new proof of Theorem 4.2.2.

c) If $f\colon\mathbb{N}\to\mathbb{C}$ is a non-zero multiplicative function, then

$$\sum_{d\,|\,n}\mu(d)f(d)=\prod_{p\,|\,n}(1-f(p))$$

(where an empty product has the value 1).

d) $\mu*\iota=\varepsilon$. In particular, $\mu*\mathsf{S}f=f$ for every multiplicative function $f\colon\mathbb{N}\to\mathbb{C}$ (Möbius inversion formula).

The study of multiplicative functions is a fascinating topic of number theory with many arithmetical applications. The interested reader should consult Elliott's book [**91**] to get an impression of this theory. The Euler product representation of series defined by multiplicative functions (as given in the next theorem) is one of the most classical and useful tools in analytic number theory.

Theorem 4.2.4 (Euler products)**.** *Let* $f\colon \mathbb{N} \to \mathbb{C}$ *be a function.*

1. *Let* f *be multiplicative. Then*

$$\sum_{n=0}^{\infty} |f(n)| = \prod_{p\in\mathbb{P}} \Bigl(\sum_{j=0}^{\infty} |f(p^j)|\Bigr) \in \mathbb{R}_{>0} \cup \{\infty\}\,,$$

and if this expression is finite, then

$$\sum_{n=0}^{\infty} f(n) = \prod_{p\in\mathbb{P}} \Bigl(\sum_{j=0}^{\infty} f(p^j)\Bigr)\,.$$

2. *Suppose that* f *is completely multiplicative,* $f(1) = 1$*, and* $|f(p)| < 1$ *for all primes* p*. Then*

$$\sum_{n=0}^{\infty} |f(n)| = \prod_{p\in\mathbb{P}} \frac{1}{1 - |f(p)|} \in \mathbb{R}_{>0} \cup \{\infty\}\,,$$

and if this expression is finite, then

$$\exp\Bigl\{\sum_{p\in\mathbb{P}} \sum_{j=1}^{\infty} \frac{f(p^j)}{j}\Bigr\} = \sum_{n=0}^{\infty} f(n) = \prod_{p\in\mathbb{P}} \frac{1}{1 - f(p)} \neq 0\,.$$

Proof. 1. For every $N \in \mathbb{N}$, we have

$$\sum_{n=1}^{N} |f(n)| \le \prod_{p\le N} \sum_{j=0}^{N} |f(p^j)| \le \sum_{n=1}^{\infty} |f(n)|\,,$$

and for $N \to \infty$, it follows that

$$\sum_{n=1}^{\infty} |f(n)| = \prod_{p\in\mathbb{P}} \sum_{j=0}^{\infty} |f(p^j)|\,.$$

Assume now that this expression is finite and let $\varepsilon > 0$ be arbitrary. Then there exists some $N_1 \in \mathbb{N}$ such that

$$\sum_{n=N_1+1}^{\infty} |f(n)| < \varepsilon\,.$$

For $N \ge N_1$, let $T(N)$ be the set of all $n \in \mathbb{N}$ not divisible by some prime $p \le N$. Then we obtain

$$\Bigl|\sum_{n=1}^{\infty} f(n) - \prod_{p\le N} \Bigl(\sum_{j=0}^{\infty} f(p^j)\Bigr)\Bigr| = \Bigl|\sum_{n\in T(N)} f(n)\Bigr| \le \sum_{n=N+1}^{\infty} |f(a)| \le \sum_{n=N_1+1}^{\infty} |f(a)| < \varepsilon\,,$$

and consequently it follows that

$$\sum_{n=1}^{\infty} f(n) = \prod_{p\in\mathbb{P}} \Big(\sum_{j=0}^{\infty} f(p^j) \Big) .$$

2. Since $|f(p)| < 1$ and $f(p^j) = f(p)^j$ for all primes p and $j \in \mathbb{N}_0$, we get

$$\sum_{n=1}^{\infty} |f(n)| = \prod_{p\in\mathbb{P}} \Big(\sum_{j=0}^{\infty} |f(p)|^j \Big) = \prod_{p\in\mathbb{P}} \frac{1}{1-|f(p)|} \in \mathbb{R}_{>0} \cup \{\infty\} .$$

If this expression is finite, then (see Appendix B.1.3)

$$\begin{aligned} 0 \ne \exp\Big\{ \sum_{p\in\mathbb{P}} \sum_{j=1}^{\infty} \frac{f(p^j)}{j} \Big\} &= \prod_{p\in\mathbb{P}} \exp\Big\{ \sum_{j=1}^{\infty} \frac{f(p^j)}{j} \Big\} \\ &= \prod_{p\in\mathbb{P}} \frac{1}{1-f(p)} = \prod_{p\in\mathbb{P}} \Big(\sum_{j=0}^{\infty} f(p)^j \Big) = \sum_{n=1}^{\infty} f(n) . \qquad \Box \end{aligned}$$

Exercise 4.2.5. Let $f\colon \mathbb{N} \to \mathbb{R}_{\ge 0}$ be a multiplicative function and $x \in \mathbb{R}_{\ge 2}$. Prove that

$$\sum_{n\le x} f(n) \le \prod_{p\le x} \sum_{\nu=0}^{\infty} f(p^\nu) \quad \text{and deduce that} \quad \log x < \prod_{p\le x} \Big(1 - \frac{1}{p} \Big)^{-1} ,$$

which implies that there are infinitely many primes (this nice argument it taken from [**14**]). Hint: Use the inequality

$$\log(n+1) < \sum_{k=1}^{n} \frac{1}{k} < 1 + \log n , \quad \text{which follows by Lemma B.2.6.}$$

Corollary 4.2.6. *Let* $\mathsf{a}\colon \mathbb{N} \to \mathbb{C}$ *be a non-zero completely multiplicative function and* $\vartheta \in \mathbb{R}_{>0}$ *such that*

$$\sum_{n=1}^{\infty} \frac{|\mathsf{a}(n)|}{n^\sigma} < \infty \quad \textit{for every } \sigma > \vartheta .$$

Let $F\colon \mathcal{H}_\vartheta \to \mathbb{C}$ *and* $W\colon \mathcal{H}_\vartheta \to \mathbb{C}$ *be the holomorphic functions defined by*

$$F(s) = \sum_{n\ge 1} \frac{\mathsf{a}(n)}{n^s} \quad \textit{and} \quad W(s) = \sum_{p\in\mathbb{P}} \sum_{j\ge 1} \frac{\mathsf{a}(p^j)}{j p^{js}} \quad (\textit{see } \text{Lemma B.2.2}).$$

Then

$$F(s) = \sum_{n=1}^{\infty} \frac{\mathsf{a}(n)}{n^s} = \prod_{p\in\mathbb{P}} \Big(1 - \frac{\mathsf{a}(p)}{p^s} \Big)^{-1} = \exp(W(s)) \quad \textit{for all} \quad s \in \mathcal{H}_\vartheta ,$$

and if a *is bounded, then the assertion holds for* $\vartheta = 1$.

PROOF. Since a is completely multiplicative, the function $f\colon \mathbb{N} \to \mathbb{C}$, defined by $f(n) = \mathsf{a}(n) n^{-s}$ is also completely multiplicative. Hence Theorem 4.2.4.2 implies the product representation of F and the relation $F = \exp(W)$. $\Box$

4.3. Dirichlet L-functions and proof of Dirichlet's theorem

This section is the core of the chapter. We introduce and investigate Dirichlet L-functions so that we can prove the theorem on primes in arithmetic progressions. We start with some useful estimates of character sums. Recall that for $m \in \mathbb{N}$ we denote by $\mathbf{1}_m \in \mathsf{X}(m)$ the unit character modulo m. In particular, $\mathbf{1} = \mathbf{1}_1$ is the constant function with value 1.

Theorem 4.3.1. *Let m be a positive integer and $\chi \in \mathsf{X}(m)$ a (Dirichlet) character modulo m.*

1. *If $k, n \in \mathbb{N}$ and $(k,m) = 1$, then*

$$\sum_{\chi \in \mathsf{X}(m)} \overline{\chi}(k)\,\chi(n) = \begin{cases} \varphi(m) & \textit{if } \ n \equiv k \mod m\,, \\ 0 & \textit{if } \ n \not\equiv k \mod m\,. \end{cases}$$

2. *For every $c \in \mathbb{Z}$ we have*

$$\sum_{n=c+1}^{c+m} \chi(n) = \begin{cases} \varphi(m) & \textit{if } \ \chi = \mathbf{1}_m\,, \\ 0 & \textit{if } \ \chi \neq \mathbf{1}_m\,, \end{cases}$$

where φ denotes Euler's function.

3. *If $\chi \neq \mathbf{1}_m$, $s, x, X \in \mathbb{R}_{>0}$ and $x < X$, then*

$$\Big|\sum_{x<n\le X} \chi(n)\Big| < m \quad \textit{and} \quad \Big|\sum_{x<n\le X} \frac{\chi(n)}{n^s}\Big| \le \frac{3m}{x^s}\,.$$

Proof. 1. If $(n,m) \neq 1$, then $n \not\equiv k \bmod m$, $\chi(n) = 0$ for all $\chi \in \mathsf{X}(m)$, and the assertion holds. Thus suppose that $(n,m) = 1$, and set $\overline{r} = r + m\mathbb{Z}$ for $r \in \mathbb{Z}$. Then we obtain (see Theorem A.7.7)

$$\begin{aligned} \sum_{\chi \in \mathsf{X}(m)} \overline{\chi}(k)\,\chi(n) &= \sum_{\chi \in \mathsf{X}(m)} \chi(\overline{k}^{-1}\overline{n}) \\ &= \begin{cases} \varphi(m) & \text{if } \ \overline{k}^{-1}\overline{n} = \overline{1} \quad (\text{that is, if } \ n \equiv k \mod m\,)\,, \\ 0 & \text{if } \ \overline{k}^{-1}\overline{n} \neq \overline{1} \quad (\text{that is, if } \ n \not\equiv k \mod m\,)\,. \end{cases} \end{aligned}$$

2. Let $c \in \mathbb{Z}$. We apply Theorem A.7.7 again and obtain

$$\sum_{n=c+1}^{c+m} \chi(n) \;=\; \sum_{t \in (\mathbb{Z}/m\mathbb{Z})^\times} \chi(t) \;=\; \begin{cases} \varphi(m) & \text{if } \ \chi = \mathbf{1}_m\,, \\ 0 & \text{if } \ \chi \neq \mathbf{1}_m\,. \end{cases}$$

3. Suppose that $\chi \neq \mathbf{1}_m$, $s, x, X \in \mathbb{R}_{>0}$, $x < X$, and set $\lfloor X \rfloor = \lfloor x \rfloor + km + r$, where $k, r \in \mathbb{N}_0$ and $r < m$. By 2., it follows that

$$\Big|\sum_{x<n\le X} \chi(n)\Big| \;\le\; \Big|\sum_{j=0}^{k-1} \sum_{n=\lfloor x \rfloor + jm+1}^{\lfloor x \rfloor + jm+m} \chi(n)\Big| + \sum_{n=\lfloor x \rfloor + km+1}^{\lfloor x \rfloor + km+r} |\chi(n)| \;= r < m\,.$$

Now Lemma B.2.4, applied with $\mathsf{a} = \chi$ and $g(\xi) = \xi^{-s}$, yields the inequality

$$\Big|\sum_{x<n\le X} \frac{\chi(n)}{n^s}\Big| \le \frac{3m}{x^s}\,. \qquad \square$$

Definition 4.3.2. Let m be a positive integer and $\chi \in \mathsf{X}(m)$ a (Dirichlet) character modulo m. We define the *Dirichlet L-function* $L(\,\cdot\,,\chi)\colon \mathcal{H}_1 \to \mathbb{C}$ and the *logarithmic L-function* $\Lambda(\,\cdot\,,\chi)\colon \mathcal{H}_1 \to \mathbb{C}$ by the Dirichlet series

$$L(s,\chi) = \sum_{n\ge1} \frac{\chi(n)}{n^s} \quad\text{and}\quad \Lambda(s,\chi) = \sum_{p\in\mathbb{P}}\sum_{j=1}^{\infty} \frac{\chi(p^j)}{jp^{js}} \quad \text{for}\ \ s \in \mathcal{H}_1\,.$$

According to Lemma B.2.2, $L(\,\cdot\,,\chi)\colon \mathcal{H}_1 \to \mathbb{C}$ and $\Lambda(\,\cdot\,,\chi)\colon \mathcal{H}_1 \to \mathbb{C}$ are holomorphic functions.

Of particular interest is the *Riemann zeta function*

$$\zeta = L(\,\cdot\,,\mathbf{1})\colon \mathcal{H}_1 \to \mathbb{C}\,, \quad \text{given by} \quad \zeta(s) = \sum_{n\ge1}\frac{1}{n^s} \quad \text{for all}\ \ s\in\mathcal{H}_1.$$

Based on our preliminary work, it is now easy to prove the analytic properties of the Dirichlet L-functions.

Theorem 4.3.3. *Let m be a positive integer and $\chi \in \mathsf{X}(m)$ a (Dirichlet) character modulo m.*

1. *If $\chi \ne \mathbf{1}_m$, then the Dirichlet L-function $L(\,\cdot\,,\chi)$ extends to a holomorphic function $L(\,\cdot\,,\chi)\colon \mathcal{H}_0 \to \mathbb{C}$.*
2. *If $s \in \mathcal{H}_1$, then*

   $$L(s,\chi) = \prod_{p\in\mathbb{P}}\Big(1-\frac{\chi(p)}{p^s}\Big)^{-1} = \exp(\Lambda(s,\chi))\,, \quad L(s,\mathbf{1}_m) = \zeta(s)\prod_{p\,|\,m}(1-p^{-s})\,,$$

   and if $s\in\mathbb{R}_{>1}$, then

   $$\prod_{\psi\in\mathsf{X}(m)} L(s,\psi) \ge 1\,.$$

3. *There exists a holomorphic function $G\colon \mathcal{H}_0 \to \mathbb{C}$ such that, for all $s\in\mathcal{H}_1$,*

   $$\zeta(s) = \prod_{p\in\mathbb{P}}\frac{1}{1-p^{-s}} = \frac{s}{s-1} + sG(s) \quad \textit{and} \quad L(s,\mathbf{1}_m) = \zeta(s)\prod_{p\,|\,m}(1-p^{-s})\,.$$

   In particular, $L(\,\cdot\,,\mathbf{1}_m)$ has an extension to a holomorphic function

   $$L(\,\cdot\,,\mathbf{1}_m)\colon \mathcal{H}_0\setminus\{1\} \to \mathbb{C}\,, \quad \textit{and} \quad \lim_{s\to1}\,(s-1)L(s,\mathbf{1}_m) = \frac{\varphi(m)}{m}\,.$$

PROOF. We have already mentioned that (due to Lemma B.2.2) the functions $L(\,\cdot\,,\chi)\colon \mathcal{H}_1 \to \mathbb{C}$ and $\Lambda(\,\cdot\,,\chi)\colon \mathcal{H}_1 \to \mathbb{C}$ are holomorphic. For $s\in\mathcal{H}_1$, the function $n \mapsto \chi(n)n^{-s}$ is completely multiplicative, and therefore Corollary 4.2.6 implies

$$L(s,\chi) = \prod_{p\in\mathbb{P}}\Big(1-\frac{\chi(p)}{p^s}\Big)^{-1} = \exp(\Lambda(s,\chi))\,.$$

In particular, it follows that

$$L(s,\mathbf{1}_m)=\zeta(s)\prod_{p\,|\,m}(1-p^{-s})\,.$$

If $s\in\mathbb{R}_{>1}$, then

$$\prod_{\psi\in\mathsf{X}(m)}L(s,\psi)=\exp\Bigg(\sum_{\psi\in\mathsf{X}(m)}\Lambda(s,\psi)\Bigg)=\exp\Bigg(\sum_{p\in\mathbb{P}}\sum_{j=1}^{\infty}\frac{1}{jp^{js}}\sum_{\psi\in\mathsf{X}(m)}\psi(p^j)\Bigg)\geq 1\,,$$

since $\exp(x)\geq 1$ for all $x\in\mathbb{R}_{\geq 0}$, and (by Theorem 4.3.1)

$$\sum_{\psi\in\mathsf{X}(m)}\psi(p^j)\in\{0,\varphi(m)\}\subset\mathbb{R}_{\geq 0}\,.$$

Now we apply Theorem B.2.5 with

$$\mathsf{A}(x)=\sum_{n\leq x}\chi(n)\quad\text{for}\quad x\in\mathbb{R}_{\geq 1}\,.$$

If $\chi\neq\mathbf{1}_m$, then $|\mathsf{A}(x)|<m$ for all $x\in\mathbb{R}_{\geq 1}$ by Theorem 4.3.1.3, hence Theorem B.2.5 applies with $\lambda=\theta=0$ and shows that $L(\,\cdot\,,\chi)$ extends to a holomorphic function $L(\,\cdot\,,\chi)\colon\mathcal{H}_0\to\mathbb{C}$.

If $m=1$, then $\chi=\mathbf{1}$ and $\mathsf{A}(x)=\lfloor x\rfloor\leq x$ for all $x\in\mathbb{R}_{>0}$, hence Theorem B.2.5 applies with $\lambda=1$ and $\theta=0$ and shows that there exists a holomorphic function $G\colon\mathcal{H}_0\to\mathbb{C}$ such that

$$\zeta(s)=L(s,\mathbf{1})=\prod_{p\in\mathbb{P}}\frac{1}{1-p^{-s}}=\frac{s}{s-1}+sG(s)\quad\text{for all}\quad s\in\mathcal{H}_1\,.$$

If $m\in\mathbb{N}$ is arbitrary and $\chi=\mathbf{1}_m$, then it is now obvious that

$$L(s,\mathbf{1}_m)=\prod_{p\nmid m}\frac{1}{1-p^{-s}}=\zeta(s)\prod_{p\,|\,m}(1-p^{-s})\quad\text{for all}\quad s\in\mathcal{H}_1\,,$$

hence

$$(s-1)L(s,\mathbf{1}_m)=(s-1)\zeta(s)\prod_{p\,|\,m}(1-p^{-s})=s\big[1+(s-1)G(s)\big]\prod_{p\,|\,m}(1-p^{-s})\,,$$

and therefore (using Theorem A.6.2)

$$\lim_{s\to 1}(s-1)L(s,\mathbf{1}_m)=\prod_{p\,|\,m}\Big(1-\frac{1}{p}\Big)=\frac{\varphi(m)}{m}\,.\qquad\square$$

Dirichlet *L*-functions (and in particular the Riemann zeta function) play a fundamental role in prime number theory. They can be extended to meromorphic functions in the whole complex plane with only a simple pole at $s=1$ if $\chi=\mathbf{1}_m$, and the distribution of their zeros controls the distribution of prime numbers. By the yet widely open famous generalized Riemann hypothesis, all zeros lie on the line $\Re(s)=1/2$. For a deeper study of all these facts we refer the reader to H. Davenport's book [**20**] and the excellent comprehensive survey of recent results by W. Narkiewicz [**84**].

Exercise 4.3.4. Let $\mu\colon \mathbb{N}\to\mathbb{C}$ be the Möbius function (see Exercise 4.2.3) and $\lambda\colon\mathbb{N}\to\mathbb{C}$ the Liouville function, defined by $\lambda(n)=(-1)^r$ if $n=p_1\cdot\ldots\cdot p_r$, where $r\in\mathbb{N}_0$ and $p_1,\ldots,p_r$ are (not necessarily distinct) primes. Prove that, for $s\in\mathbb{R}_{>1}$, the following identities hold:

$$\frac{1}{\zeta(s)}=\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}=\prod_{p\in\mathbb{P}}(1-p^{-s})\,,\qquad \frac{\zeta(2s)}{\zeta(s)}=\sum_{n=1}^{\infty}\frac{\lambda(n)}{n^s}=\prod_{p\in\mathbb{P}}\frac{1}{1+p^{-s}}\,,$$

and

$$\frac{\zeta(s-1)}{\zeta(s)}=\sum_{n=1}^{\infty}\frac{\varphi(n)}{n^s}=\prod_{p\in\mathbb{P}}\frac{1-p^{-s}}{1-p^{1-s}}\,.$$

The crucial fact for the proof of Dirichlet's prime number theorem is the non-vanishing of Dirichlet's L-functions at $s=1$, to be proved in Theorem 4.3.5, and the behavior of the logarithmic L-function as $s\to 1+$, which is explained in Theorem 4.3.6.

Theorem 4.3.5. *If $m\in\mathbb{N}$ and $\chi\in\mathsf{X}(m)\setminus\{\mathbf{1}_m\}$ is a non-trivial (Dirichlet) character modulo m, then $L(1,\chi)\ne 0$.*

PROOF. Assume to the contrary that $L(1,\psi)=0$ for some positive integer m and $\psi\in\mathsf{X}(m)\setminus\{\mathbf{1}_m\}$.

CASE 1: $\psi\ne\overline{\psi}$. Then $\overline{\psi}\in\mathsf{X}(m)$, and $L(s,\overline{\psi})=\overline{L(s,\psi)}$ for all $s\in\mathbb{R}_{>0}$. Since $L(\,\cdot\,,\psi)$ is differentiable in 1, there exists a continuous function $G\colon\mathbb{R}_{>0}\to\mathbb{C}$ such that $L(s,\psi)=(s-1)G(s)$ and thus $L(s,\overline{\psi})=(s-1)\overline{G(s)}$ for all $s\in\mathbb{R}_{>0}$. By Theorem 4.3.3.2, it follows that

$$1\le\prod_{\chi\in\mathsf{X}(m)}L(s,\chi)=L(s,\mathbf{1}_m)L(s,\psi)L(s,\overline{\psi})F(s)=L(s,\mathbf{1}_m)(s-1)^2|G(s)|^2F(s)$$

for all $s\in\mathbb{R}_{>1}$, where

$$F(s)=\prod_{\chi\in\mathbf{X}(m)\setminus\{\mathbf{1}_m,\psi,\overline{\psi}\}}L(s,\chi)\,,$$

and $F\colon\mathbb{R}_{>0}\to\mathbb{C}$ is a differentiable function. Since

$$\lim_{s\to1+}(s-1)|G(s)|^2F(s)=0\quad\text{and}\quad\lim_{s\to1+}(s-1)L(s,\mathbf{1}_m)=\frac{\varphi(m)}{m}$$

(by Theorem 4.3.3), we arrive at a contradiction.

CASE 2: $\psi=\overline{\psi}$. Let $\Phi\colon\mathbb{N}\to\mathbb{R}$ and $\Psi\colon\mathbb{R}_{\ge0}\to\mathbb{R}$ be defined by

$$\Phi(n)=\sum_{1\le d\,|\,n}\psi(d)\quad\text{and}\quad\Psi(x)=\sum_{n\le x}\frac{\Phi(n)}{\sqrt{n}}\,.$$

By Theorem 4.2.2, Φ is multiplicative. If p is a prime and $e\in\mathbb{N}_0$, then

$$\Phi(p^e)=\sum_{j=0}^{e}\psi(p)^j=\begin{cases}e+1 & \text{if}\quad \psi(p)=1\,,\\ 1 & \text{if}\quad\psi(p)=-1\ \text{ and }\ e\text{ is even}\,,\\ 0 & \text{if}\quad p\,|\,m\,.\end{cases}$$

Hence it follows that $\Phi(n) \ge 0$ for all $n \in \mathbb{N}$, and $\Phi(n^2) \ge 1$ for all $n \in \mathbb{N}$ such that $(m,n) = 1$. For $x \in \mathbb{R}_{>1}$, we obtain

$$\Psi(x) = \sum_{n \le x} \frac{\Phi(n)}{\sqrt{n}} \ge \sum_{n \le \sqrt{x}} \frac{\Phi(n^2)}{n} \ge \sum_{\substack{n \le \sqrt{x} \\ (n,m)=1}} \frac{1}{n} \ge \sum_{\substack{n \ge 1 \\ mn+1 \le \sqrt{x}}} \frac{1}{mn+1}\,,$$

and therefore

$$\lim_{x \to \infty} \Psi(x) = \infty\,.$$

Let $x \in \mathbb{R}_{\ge 1}$. By the Theorems 4.3.1 and 4.3.3.4, it follows that

$$\sum_{n \ge 1} \frac{\psi(n)}{n} \quad \text{converges,} \qquad \Bigl|\sum_{n > x} \frac{\psi(n)}{n}\Bigr| = \lim_{X \to \infty} \Bigl|\sum_{x < n \le X} \frac{\psi(n)}{n}\Bigr| \le \frac{3m}{x}\,,$$

and

$$\Bigl|\sum_{d \le x} \frac{\psi(d)}{d}\Bigr| = \Bigl|L(1,\psi) - \sum_{d > x} \frac{\psi(d)}{d}\Bigr| = \Bigl|\sum_{d > x} \frac{\psi(d)}{d}\Bigr| \le \frac{3m}{x}\,.$$

If $(d, d') \in \mathbb{N}^2$, then $dd' \le x$ if and only if

$$\text{either} \quad d' \le \sqrt{x} \quad \text{and} \quad \sqrt{x} < d \le \frac{x}{d'}\,, \qquad \text{or} \quad d \le \sqrt{x} \quad \text{and} \quad d' \le \frac{x}{d}\,,$$

and therefore

$$\begin{aligned}\Psi(x) &= \sum_{n \le x} \sum_{d \,|\, n} \frac{\psi(d)}{\sqrt{n}} = \sum_{\substack{d,\, d' \ge 1 \\ dd' \le x}} \frac{\psi(d)}{\sqrt{d}\sqrt{d'}} \\ &= \sum_{d' \le \sqrt{x}} \frac{1}{\sqrt{d'}} \sum_{\sqrt{x} < d \le \frac{x}{d'}} \frac{\psi(d)}{\sqrt{d}} + \sum_{d \le \sqrt{x}} \frac{\psi(d)}{\sqrt{d}} \sum_{d' \le \frac{x}{d}} \frac{1}{\sqrt{d'}}\,.\end{aligned}$$

Using Theorem 4.3.1.3 and Lemma B.2.6, we obtain

$$\begin{aligned}\Bigl|\sum_{d' \le \sqrt{x}} \frac{1}{\sqrt{d'}} \sum_{\sqrt{x} \le d \le \frac{x}{d'}} \frac{\psi(d)}{\sqrt{d}}\Bigr| &\le \sum_{d' \le \sqrt{x}} \frac{1}{\sqrt{d'}} \frac{3m}{x^{1/4}} \le \frac{3m}{x^{1/4}} \Bigl[\int_1^{\sqrt{x}} \frac{d\xi}{\sqrt{\xi}} + 1\Bigr] \\ &= \frac{3m}{x^{1/4}} \bigl[2x^{1/4} - 2 + 1\bigr] < 6m\,.\end{aligned}$$

If $y \in \mathbb{R}_{\ge 1}$, then Lemma B.2.6 implies

$$\sum_{n \le y} \frac{1}{\sqrt{y}} = \int_1^y \frac{d\xi}{\sqrt{\xi}} + \theta(y) = 2\sqrt{y} - 2 + \theta(y)\,, \quad \text{where} \quad 0 \le \theta(y) \le 1\,,$$

hence $|-2+\theta(y)| \le 2$, and therefore

$$\begin{aligned}\Big|\sum_{d\le\sqrt{x}} \frac{\psi(d)}{\sqrt{d}} \sum_{d'\le\frac{x}{d}} \frac{1}{\sqrt{d'}}\Big| &= \Big|\sum_{d\le\sqrt{x}} \frac{\psi(d)}{\sqrt{d}} \Big[2\sqrt{\frac{x}{d}} - 2 + \theta\Big(\frac{x}{d}\Big)\Big]\Big| \\ &\le 2\sqrt{x}\Big|\sum_{d\le\sqrt{x}} \frac{\psi(d)}{d}\Big| + 2\Big|\sum_{d\le\sqrt{x}} \frac{\psi(d)}{\sqrt{d}}\Big| \\ &\le 2\sqrt{x}\,\frac{3m}{\sqrt{x}} \;+\; 2\Big|\sum_{d\le\sqrt{x}} \frac{\psi(d)}{\sqrt{d}}\Big| \;\le 12m\,.\end{aligned}$$

Now it follows that $\Psi(x) \le 18m$ for all $x \in \mathbb{R}_{\ge 1}$, a contradiction. □

Theorem 4.3.6. *Let m be a positive integer and $\chi \in \mathsf{X}(m)$. For $s \in \mathbb{R}_{>1}$, the logarithmic L-functions behave as follows for $s \to 1$:*

$$\lim_{s\to 1+} \Lambda(s,\chi) \;\; \textit{exists in } \mathbb{C} \;\; \textit{if} \;\; \chi \ne \mathbf{1}_m, \;\; \textit{and} \;\; \lim_{s\to 1+} \Lambda(s,\mathbf{1}_m) = \infty\,.$$

Proof. Theorem 4.3.3.1 implies

$$\lim_{s\to 1+} (s-1)L(s,\mathbf{1}_m) = \frac{\varphi(m)}{m}\,, \quad \text{hence} \quad \lim_{s\to 1+} L(s,\mathbf{1}_m) = \infty\,.$$

If $s \in \mathbb{R}_{>1}$, then $\Lambda(s,\mathbf{1}_m) \in \mathbb{R}$, $L(s,\mathbf{1}_m) = \exp\Lambda(s,\mathbf{1}_m)$, and therefore

$$\lim_{s\to 1+} \Lambda(s,\mathbf{1}_m) = \infty\,.$$

Assume now that $\chi \ne \mathbf{1}_m$. Then $L(1,\chi) \ne 0$ by Theorem 4.3.5, hence there exists some $b \in \mathbb{C}$ such that $L(1,\chi) = \mathsf{e}^b$, and we define

$$h\colon \mathbb{R}_{>1} \to \mathbb{C} \quad \text{by} \quad h(s) = 1 - \mathsf{e}^{-b}L(s,\chi)\,.$$

Since $L(\,\cdot\,,\chi)\colon \mathbb{R}_{>0} \to \mathbb{C}$ is continuous, there exist $\varepsilon,\,\theta \in (0,1)$ such that $|h(s)| \le \theta$ for all $s \in (1-\varepsilon, 1+\varepsilon)$, h is continuous, and we define $H\colon (1-\varepsilon,1+\varepsilon) \to \mathbb{C}$ by

$$H(s) = \sum_{j=1}^{\infty} \frac{h(s)^j}{j}\,.$$

This series is uniformly convergent, hence H is continuous, and if $s \in (1, 1+\varepsilon)$, then

$$\mathsf{e}^{H(s)} = \frac{1}{1-h(s)} = \frac{\mathsf{e}^b}{L(s,\chi)} = \mathsf{e}^{b-\Lambda(s,\chi)}\,.$$

The function $K\colon (1,1+\varepsilon) \to \mathbb{C}$, defined by $K(s) = H(s) - b + \Lambda(s,\chi)$, is continuous, and as $\mathsf{e}^{K(s)} = 1$, it follows that $K(s) \in 2\pi\mathsf{i}\mathbb{Z}$ or all $s \in (1, 1+\varepsilon)$. Hence K is constant, say $K(s) = c \in \mathbb{C}$ for all $s \in (1, 1+\varepsilon)$, and

$$\lim_{s\to 1+} \Lambda(s,\chi) = \lim_{s\to 1+} [\,K(s) - H(s) + b\,] = c - H(1) + b \in \mathbb{C}\,.$$

□

Proof of Theorem 4.1.1 (Dirichlet's prime number theorem).
Let k and m be positive integers such that $(k,m)=1$. For $s\in\mathbb{R}_{>1}$, we consider the series

$$\pi(s)=\sum_{\substack{p\in\mathbb{P}\\ p\equiv k \bmod m}}\frac{1}{p^s}\quad\text{and}\quad \Pi(s)=\sum_{\chi\in\mathsf{X}(m)}\overline{\chi}(k)\Lambda(s,\chi)\,.$$

Using Theorem 4.3.1.2, we obtain

$$\begin{aligned}\Pi(s)&=\sum_{p\in\mathbb{P}}\sum_{\chi\in\mathsf{X}(m)}\overline{\chi}(k)\chi(p)p^{-s}+\sum_{p\in\mathbb{P}}\sum_{j=2}^{\infty}\sum_{\chi\in\mathsf{X}(m)}\overline{\chi}(k)\chi(p^j)p^{-sj}\\ &=\varphi(m)\,\pi(s)\;+\sum_{\chi\in\mathsf{X}(m)}G_\chi(s)\,,\quad\text{where}\quad G_\chi(s)=\sum_{p\in\mathbb{P}}\sum_{j=2}^{\infty}\overline{\chi}(k)\chi(p^j)p^{-sj}\,.\end{aligned}$$

If $\chi\in\mathsf{X}(m)$, $\frac12<\vartheta<1$ and $s\ge\vartheta$, then

$$|G_\chi(s)|\;\le\;\sum_{p\in\mathbb{P}}\sum_{j=2}^{\infty}\frac{1}{p^{\vartheta j}}\;=\;\sum_{p\in\mathbb{P}}\frac{1}{p^{2\vartheta}}\,\frac{1}{1-p^{-\vartheta}}\;\le\;\frac{1}{1-2^{-\vartheta}}\sum_{p\in\mathbb{P}}\frac{1}{p^{2\vartheta}}\;<\infty\,.$$

Hence the series defining G_χ are absolutely and uniformly convergent in $\mathbb{R}_{\ge\vartheta}$, and therefore the functions G_χ are continuous in 1. For $s\in\mathbb{R}_{>1}$, we obtain

$$\pi(s)=\frac{1}{\varphi(m)}\,[\Lambda(s,\mathbf{1}_m)+H(s)]\,,\quad\text{where}\quad H(s)=\sum_{\substack{\chi\in\mathsf{X}(m)\\ \chi\ne\mathbf{1}_m}}\overline{\chi}(k)\Lambda(s,\chi)+\sum_{\chi\in\mathsf{X}(m)}G_\chi(s)\,.$$

By Theorem 4.3.6,

$$\lim_{s\to1+}H(s)\ \text{exists in }\mathbb{C}\quad\text{and}\quad\lim_{s\to1+}\Lambda(s,\mathbf{1}_m)=\infty\,,\quad\text{hence}\quad\lim_{s\to1+}\pi(s)=\infty\,,$$

and therefore the set $\{p\in\mathbb{P}\mid p\equiv k \bmod m\}$ is infinite. □

4.4. Summation of L-series

For later use (in Chapter 8), we apply our analytical skills to derive a finite expression for $L(1,\chi)$ for primitive (Dirichlet) characters $\chi\in\mathsf{X}(m)\setminus\{\mathbf{1}_m\}$. We make use of the series expansion of the principal branch of the complex logarithm $\log\colon\mathbb{C}\setminus R_{\le0}\to\mathbb{C}$, given by

$$\log(r\mathsf{e}^{\mathsf{i}\phi})=\log r+\mathsf{i}\phi\quad\text{for all }\ r\in\mathbb{R}_{>0}\ \text{and}\ \phi\in(-\pi,\pi).$$

If $z\in\mathbb{C}\setminus\{1\}$ and $|z|\le1$, then $\Re(1-z)>0$, hence

$$1-z=|1-z|\mathsf{e}^{\mathsf{i}\phi}\,,\quad\phi\in\Bigl(-\frac{\pi}{2},\frac{\pi}{2}\Bigr),\quad\text{and}\quad\log(1-z)=-\sum_{n=1}^{\infty}\frac{z^n}{n}=\log|1-z|+\mathsf{i}\,\phi\,.$$

In the following Lemma 4.4.1 we prove a refinement of this relation.

Lemma 4.4.1. *If* $m \in \mathbb{N}$ *and* $j \in [1, m-1]$, *then*

$$\sum_{n=1}^{\infty} \frac{\zeta_m^{jn}}{n} = \log(1-\zeta_m^j) = \log\Bigl(2\sin\frac{\pi j}{m}\Bigr) + \mathsf{i}\Bigl(-\frac{\pi}{2} + \frac{\pi j}{m}\Bigr)$$

and

$$\sum_{n=1}^{\infty} \frac{\zeta_m^{-jn}}{n} = \log(1-\zeta_m^{-j}) = \log\Bigl(2\sin\frac{\pi j}{m}\Bigr) - \mathsf{i}\Bigl(-\frac{\pi}{2} + \frac{\pi j}{m}\Bigr).$$

Proof. We have

$$1-\zeta_m^j = -\zeta_{2m}^j(\zeta_{2m}^j - \zeta_{2m}^{-j}) = -\zeta_{2m}^j\Bigl(2\mathsf{i}\,\sin\frac{\pi j}{m}\Bigr) = \Bigl(2\sin\frac{\pi j}{m}\Bigr)\mathsf{e}^{\mathsf{i}(-\frac{\pi}{2}+\frac{\pi j}{m})}$$

and

$$1-\zeta_m^{-j} = \overline{1-\zeta_m^j} = \Bigl(2\sin\frac{\pi j}{m}\Bigr)\mathsf{e}^{-\mathsf{i}(-\frac{\pi}{2}+\frac{\pi j}{m})}\,.$$

Since

$$\sin\frac{\pi j}{m} > 0 \quad\text{and}\quad \pm\Bigl(-\frac{\pi}{2} + \frac{j\pi}{m}\Bigr) \in \Bigl(-\frac{\pi}{2}, \frac{\pi}{2}\Bigr)\,,$$

the assertions follow. □

Theorem 4.4.2. *Let* m *be a positive integer and* $\chi \in \mathsf{X}(m) \setminus \{\mathbf{1}_m\}$ *a primitive* (*Dirichlet*) *character modulo* m. *Then*

$$L(1,\chi) = \frac{-\tau(\chi)}{m} \sum_{j=1}^{m-1} \overline{\chi}(j) \log\Bigl(\sin\frac{\pi j}{m}\Bigr) \quad \textit{if} \quad \chi(-1) = 1\,,$$

and

$$L(1,\chi) = \frac{\mathsf{i}\pi\,\tau(\chi)}{m^2} \sum_{j=1}^{m-1} \overline{\chi}(j) j \quad \textit{if} \quad \chi(-1) = -1\,.$$

Proof. We tacitly use the Theorems 3.2.1 and A.7.7. For $s \in \mathbb{R}_{>1}$ we obtain (using absolute convergence)

$$\begin{aligned} L(s,\chi) &= \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \sum_{k=1}^{m-1} \chi(k) \sum_{\substack{n=1 \\ n\equiv k \bmod m}}^{\infty} \frac{1}{n^s} = \sum_{k=1}^{m-1} \chi(k) \sum_{n=1}^{\infty} \Bigl(\frac{1}{m}\sum_{j=0}^{m-1} \zeta_m^{(n-k)j}\Bigr)\frac{1}{n^s} \\ &= \frac{1}{m}\sum_{j=0}^{m-1}\sum_{k=1}^{m-1} \chi(k)\zeta_m^{-kj} \sum_{n=1}^{\infty} \frac{\zeta_m^{jn}}{n^s} = \frac{1}{m}\sum_{j=1}^{m-1} \tau(\chi,-j) \sum_{n=1}^{\infty} \frac{\zeta_m^{jn}}{n^s}\,, \end{aligned}$$

since (for $j = 0$)

$$\sum_{k=0}^{m-1} \chi(k) = 0 \quad\text{as}\quad \chi \neq \mathbf{1}_m\,.$$

For $j \in [1, m-1]$, we have

$$\tau(\chi,-j) = \chi(-1)\overline{\chi}(j)\tau(\chi) \quad\text{and}\quad \sum_{n=1}^{\infty} \frac{\zeta_m^{jn}}{n} = -\log(1-\zeta_m^j)\,,$$

and therefore

$$L(1,\chi) = \frac{-\chi(-1)\tau(\chi)}{m}\sum_{j=1}^{m-1}\overline{\chi}(j)\log(1-\zeta_m^j)\,.$$

Using the substitution $(j \mapsto -j)$, we get

$$L(1,\chi) = \frac{-\chi(-1)\tau(\chi)}{m}\sum_{j=1}^{m-1}\overline{\chi}(-j)\log(1-\zeta_m^{-j}) = \frac{-\tau(\chi)}{m}\sum_{j=1}^{m-1}\overline{\chi}(j)\log(1-\zeta_m^{-j})\,,$$

and therefore

$$2L(1,\chi) = \frac{-\tau(\chi)}{m}\sum_{j=1}^{m-1}\overline{\chi}(j)\big[\chi(-1)\log(1-\zeta_m^j) \,+\, \log(1-\zeta_m^{-j})\big]\,.$$

Now we use Lemma 4.4.1. If $\chi(-1)=1$, then

$$\log(1-\zeta_m^j) \,+\, \log(1-\zeta_m^{-j}) = 2\log\Big(2\sin\frac{\pi j}{m}\Big) = 2\log 2 \,+\, 2\log\Big(\sin\frac{\pi j}{m}\Big)\,,$$

and therefore

$$L(1,\chi) = \frac{-\tau(\chi)}{m}\sum_{j=1}^{m-1}\overline{\chi}(j)\log\Big(\sin\frac{\pi j}{m}\Big)\,, \quad \text{since} \quad \sum_{j=1}^{m-1}\overline{\chi}(j) = 0\,.$$

If $\chi(-1)=-1$, then

$$-\log(1-\zeta_m^j) \,+\, \log(1-\zeta_m^{-j}) = 2\mathsf{i}\pi\Big(\frac{1}{2}-\frac{j}{m}\Big)\,,$$

and therefore

$$L(1,\chi) = \frac{\mathsf{i}\pi\tau(\chi)}{m^2}\sum_{j=1}^{m-1}\overline{\chi}(j)j\,, \quad \text{since} \quad \sum_{j=1}^{m-1}\overline{\chi}(j) = 0\,. \qquad \square$$

CHAPTER 5

Quadratic orders

We have already introduced quadratic number fields and their discriminants in Chapter 1 (see Definition 1.1.8 and Theorem 1.1.9). In this chapter we introduce and investigate lattices and orders in quadratic number fields as well as ideals and ideal classes. These are the basic algebraic objects built by quadratic irrationals. Their structure will be the basis for a deeper understanding of Gauss' theory of binary quadratic forms in Chapter 6. Apart from that, the algebraic theory of quadratic orders is of independent interest, and we shall investigate it in detail.

Several aspects of the theory are dealt with in many books on elementary and algebraic number theory. The main references for the treatment in this volume are the books [**19**], [**16**], [**74**] and the articles [**58**] and [**40**].

5.1. Lattices and orders in quadratic number fields

Let K be a quadratic number field. The map $\iota\colon K \to K$, defined by $\iota(\xi) = \xi'$ for all $\xi \in K$, is a field automorphism satisfying $\iota\,|\,\mathbb{Q} = \mathrm{id}_{\mathbb{Q}}$ (see Theorem 1.1.9). Recall that $(u+v\sqrt{d})' = u - v\sqrt{d}$ if u, v, $d \in \mathbb{Q}$ and d is not a square. The *norm* and the *trace* of an element $\alpha \in K$ are defined by $\mathcal{N}(\alpha) = \alpha\alpha'$ and $\mathcal{T}(\alpha) = \alpha + \alpha'$, and for any subset $X \subset K$, we set $X' = \{\alpha' \mid \alpha \in X\}$. For a subring R of K, we write $\mathsf{q}(R) = K$ if K is a quotient field of R.

A *lattice* (in K) is a finitely generate subgroup $\mathfrak{a}$ of K such that $\mathbb{Q}\mathfrak{a} = K$. A reader not familiar with this notion of Diophantine linear algebra should consult Section A.4 for a thorough treatment of the subject. Here we only consider two-dimensional lattices in quadratic number fields. By Corollary A.4.3, the following assertions are equivalent for a subgroup $\mathfrak{a}$ of K:

- $\mathfrak{a}$ is a lattice (in K).
- $\mathfrak{a}$ is finitely generated and contains a basis of K.
- $\mathfrak{a}$ is finitely generated, and for every $z \in K$ there is some $m \in \mathbb{N}$ such that $mz \in \mathfrak{a}$.
- $\mathfrak{a}$ has a basis consisting of two elements. Explicitly, there exists a linearly independent pair $(\omega_1, \omega_2) \in K^2$ such that
$$\mathfrak{a} = [\omega_1, \omega_2] = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2\,.$$

We shall frequently use the fact that every subgroup of a lattice is finitely generated (see Theorem A.4.2.2).

For two lattices $\mathfrak{a}$ and $\mathfrak{b}$ in K, we define the product $\mathfrak{ab}$ and the quotient $(\mathfrak{a}:_K \mathfrak{b})$ by

$$\mathfrak{ab} = \Big\{ \sum_{i=1}^{n} a_i b_i \;\Big|\; n \in \mathbb{N},\ a_i \in \mathfrak{a},\ b_i \in \mathfrak{b} \Big\} \quad \text{and} \quad (\mathfrak{a}:_K \mathfrak{b}) = \{\alpha \in K \mid \alpha\mathfrak{b} \subset \mathfrak{a}\}\,.$$

Lemma 5.1.1. *Let K be a quadratic number field. If $\mathfrak{a}$ and $\mathfrak{b}$ are lattices in K and $\lambda \in K^\times$, then*

$$\mathfrak{a}',\ \lambda\mathfrak{a},\ \mathfrak{a}+\mathfrak{b},\ \mathfrak{a}\cap\mathfrak{b},\ \mathfrak{ab} \ \ \textit{and} \ \ (\mathfrak{a}:_K \mathfrak{b})$$

are also lattices in K, and if $\alpha,\ \beta \in K^\times$, then $(\alpha\mathfrak{a}:_K \beta\mathfrak{b}) = \alpha\beta^{-1}(\mathfrak{a}:_K \mathfrak{b})$.

Addition and multiplication of lattices in K are commutative and associative laws of composition, and the distributive law $\mathfrak{a}(\mathfrak{b}+\mathfrak{c}) = \mathfrak{ab}+\mathfrak{ac}$ hold for all lattices $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ in K. In particular, the set $\mathcal{L}(K)$ of all lattices in K is a commutative multiplicative semigroup (and even a semiring).

Proof. Suppose that $\mathfrak{a} = [\omega_1, \omega_2]$ and $\mathfrak{b} = [\eta_1, \eta_2]$. Since $\alpha \mapsto \alpha'$ is an automorphism of K, it follows that $\mathfrak{a}'$ is a lattice, and obviously $\lambda\mathfrak{a} = [\lambda\omega_1, \lambda\omega_2]$ is also a lattice.

$\mathfrak{a}+\mathfrak{b} = [\omega_1, \omega_2, \eta_1, \eta_2]$ is a finitely generated subgroup of K and contains the basis (ω_1, ω_2) of K, and $\mathfrak{ab} = [\omega_1\eta_1, \omega_2\eta_1, \omega_1\eta_2, \omega_2\eta_2]$ is a finitely generated subgroup of K and contains the basis $(\omega_1\eta_1, \omega_1\eta_2)$ of K. Hence $\mathfrak{a}+\mathfrak{b}$ and $\mathfrak{ab}$ are lattices in K.

Since $\mathfrak{a}\cap\mathfrak{b} \subset \mathfrak{a}$, it follows that $\mathfrak{a}\cap\mathfrak{b}$ is finitely generated. If $z \in K$ and $m_1,\ m_2 \in \mathbb{N}$ are such that $m_1 z \in \mathfrak{a}$ and $m_2 z \in \mathfrak{b}$, then $m_1 m_2 z \in \mathfrak{a}\cap\mathfrak{b}$. Hence $\mathfrak{a}\cap\mathfrak{b}$ is a lattice.

If $\alpha \in K$, then $\alpha \in (\mathfrak{a}:_K \mathfrak{b})$ holds if and only if $\{\alpha\eta_1, \alpha\eta_2\} \subset \mathfrak{a}$, and therefore $(\mathfrak{a}:_K \mathfrak{b}) = \eta_1^{-1}\mathfrak{a} \cap \eta_2^{-1}\mathfrak{a}$ is a lattice.

If $\alpha,\ \beta \in K^\times$ and $x \in K$, then we obtain:

$$\begin{aligned} x \in (\alpha\mathfrak{a}:_K \beta\mathfrak{b}) \iff{}& x\beta\mathfrak{b} \subset \alpha\mathfrak{a} \iff \alpha^{-1}\beta x\mathfrak{b} \subset \mathfrak{a} \iff \alpha^{-1}\beta x \in (\mathfrak{a}:_K \mathfrak{b}) \\ \iff{}& x \in \alpha\beta^{-1}(\mathfrak{a}:_K \mathfrak{b})\,. \end{aligned}$$

Hence it follows that $(\alpha\mathfrak{a}:_K \beta\mathfrak{b}) = \alpha\beta^{-1}(\mathfrak{a}:_K \mathfrak{b})$. The commutative, associative and distributive laws are easily checked. $\square$

Exercise 5.1.2. Prove the following relations for lattices $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ in a quadratic number field K, and discuss in which more general (ring-theoretical) context these relations hold:

- $((\mathfrak{a}:_K \mathfrak{b}):_K \mathfrak{c}) = (\mathfrak{a}:_K \mathfrak{bc})$;
- $(\mathfrak{a}:_K (\mathfrak{b}+\mathfrak{c})) = (\mathfrak{a}:_K \mathfrak{b}) \cap (\mathfrak{a}:_K \mathfrak{c})$ and $((\mathfrak{a}\cap\mathfrak{b}):_K \mathfrak{c}) = (\mathfrak{a}:_K \mathfrak{c}) \cap (\mathfrak{b}:_K \mathfrak{c})$;
- If $\mathfrak{a} \subset \mathfrak{c}$, then

$$(\mathfrak{a}:_K \mathfrak{b}) \subset (\mathfrak{c}:_K \mathfrak{b}),\ \ (\mathfrak{b}:_K \mathfrak{c}) \subset (\mathfrak{b}:_K \mathfrak{a}) \quad \text{and} \quad \mathfrak{a} + (\mathfrak{b}\cap\mathfrak{c}) = (\mathfrak{a}+\mathfrak{b}) \cap \mathfrak{c}.$$

Theorem 5.1.3. *Let K be a quadratic number field, $\xi \in K^\times$, and let $\mathfrak{a}$ and $\mathfrak{c}$ be lattices in K such that $\mathfrak{a} \subset \mathfrak{c}$ and $\xi\mathfrak{a} \subset \mathfrak{c}$. Then*

$$(\mathfrak{c}:_K \xi\mathfrak{a}) = |\mathcal{N}(\xi)|(\mathfrak{c}:_K \mathfrak{a})\,.$$

Proof. Suppose that $\mathfrak{c} = [\eta_1, \eta_2]$ and $\mathfrak{a} = [\omega_1, \omega_2]$. Then $\xi\mathfrak{a} = [\xi\omega_1, \xi\omega_2]$, and by Lemma A.4.1 there exist matrices A, $B \in \mathsf{M}_2(\mathbb{Z}) \cap \mathsf{GL}_2(\mathbb{Q})$ such that

$$\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix} = A\begin{pmatrix}\eta_1\\ \eta_2\end{pmatrix} \quad\text{and}\quad \begin{pmatrix}\xi\omega_1\\ \xi\omega_2\end{pmatrix} = B\begin{pmatrix}\eta_1\\ \eta_2\end{pmatrix}\,, \quad\text{which implies}\ \ \xi\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix} = BA^{-1}\begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix}.$$

It follows that $(\mathfrak{c}\,{:}_K\,\mathfrak{a}) = |\det(A)|$, $(\mathfrak{c}\,{:}_K\,\xi\mathfrak{a}) = |\det(B)|$ (see Theorem A.4.2.4), and ξ is a zero of the characteristic polynomial

$$g = \det(XI - BA^{-1}) = X^2 - \mathrm{Sp}(BA^{-1})X + \det(BA^{-1}) \in \mathbb{Q}[X]\,.$$

Hence $\mathcal{N}(\xi) = \det(BA^{-1})$, and

$$(\mathfrak{c}\,{:}_K\,\xi\mathfrak{a}) = |\det(B)| = |\mathcal{N}(\xi)|\,|\det(A)| = |\mathcal{N}(\xi)|(\mathfrak{c}\,{:}_K\,\mathfrak{a})\,. \qquad \square$$

Exercise 5.1.4. Let K be a quadratic number field. For a pair $(\xi_1, \xi_2) \in K^2$, we define $\partial(\xi_1, \xi_2) = (\xi_1\xi_2' - \xi_1'\xi_2)^2$.

a) Prove that $\partial(\xi_1, \xi_2) = 0$ if and only if (ξ_1, ξ_2) is linearly dependent.

b) Let $\mathfrak{a} = [\omega_1, \omega_2]$ be a lattice in K. Prove that $\partial(\mathfrak{a}) = \partial(\omega_1, \omega_2)$ only depends on $\mathfrak{a}$. It is called the *discriminant* of $\mathfrak{a}$.

c) Let $\mathfrak{a}$ and $\mathfrak{b}$ be lattices in K, $\mathfrak{a} \subset \mathfrak{b}$ and $\lambda \in K^\times$. Prove that

$$\partial(\mathfrak{a}) = \partial(\mathfrak{b})(\mathfrak{b}\,{:}_K\,\mathfrak{a})^2 \quad\text{and}\quad \partial(\lambda\mathfrak{a}) = \mathcal{N}(\lambda)^2\partial(\mathfrak{a})\,.$$

A subring of a quadratic number field K is called an *order* (in K) if it is a lattice in K. By a *quadratic order* we mean an order in a quadratic number field. For a lattice $\mathfrak{a}$ in a quadratic number field K, we call

$$\mathcal{R}(\mathfrak{a}) = (\mathfrak{a}\,{:}_K\,\mathfrak{a}) = \{\lambda \in K \mid \lambda\mathfrak{a} \subset \mathfrak{a}\}$$

the *ring of multipliers* of $\mathfrak{a}$.

After some preparations, we shall prove in Theorem 5.1.12 the following properties of orders in a quadratic number field K :

- A subset of K is an order in K if and only if it is the ring of multipliers of a lattice in K.
- There is a natural one-to-one correspondence between the orders in K and the quadratic discriminants with associated fundamental discriminant Δ_K.

Theorem 5.1.5. *Let K be a quadratic number field, let $\mathfrak{a}$ and $\mathfrak{b}$ be lattices in K and $\lambda \in K^\times$.*

1. *$\mathcal{R}(\mathfrak{a})$ is an order in K, $\mathcal{R}(\lambda\mathfrak{a}) = \mathcal{R}(\mathfrak{a})$ and $\mathcal{R}(\mathfrak{a}) \subset \mathcal{R}(\mathfrak{a}\mathfrak{b})$.*
2. *If R is an order in K, then $\mathsf{q}(R) = K$, $\mathcal{R}(R) = R$, and every non-zero ideal of R is a lattice in K.*

Proof. 1. By Lemma 5.1.1, $\mathcal{R}(\mathfrak{a}) = (\mathfrak{a}\,{:}_K\,\mathfrak{a})$ is a lattice in K. If x, $y \in \mathcal{R}(\mathfrak{a})$, then $(x-y)\mathfrak{a} \subset x\mathfrak{a}+y\mathfrak{a} \subset \mathfrak{a}$ and $xy\mathfrak{a} \subset x\mathfrak{a} \subset \mathfrak{a}$, hence $\{x-y,\, xy\} \subset \mathcal{R}(\mathfrak{a})$. Therefore $\mathcal{R}(\mathfrak{a})$ is a subring of K and thus an order in K.

If $\alpha \in K$, then $\alpha\mathfrak{a} \subset \mathfrak{a}$ if and only if $\alpha\lambda\mathfrak{a} \subset \lambda\mathfrak{a}$, and $\alpha\mathfrak{a} \subset \mathfrak{a}$ implies $\alpha\mathfrak{a}\mathfrak{b} \subset \mathfrak{a}\mathfrak{b}$. Hence it follows that $\mathcal{R}(\lambda\mathfrak{a}) = \mathcal{R}(\mathfrak{a}) \subset \mathcal{R}(\mathfrak{a}\mathfrak{b})$.

2. Let R be an order in K. Then $RR = R$ implies $R \subset \mathcal{R}(R)$, and since obviously $\mathcal{R}(R) \subset \mathcal{R}(R)R \subset R$, we get $\mathcal{R}(R) = R$. As R is a lattice, it follows that for every $z \in K$ there is some $m \in \mathbb{Z}$ such that $mz \in R$, and $\mathbb{Z} \subset R$ implies $\mathsf{q}(R) = K$.

Let $\mathfrak{a}$ be a non-zero ideal of R. Being a subgroup of R, $\mathfrak{a}$ is finitely generated. If (ω_1, ω_2) is a basis of R and $\alpha \in \mathfrak{a}^\bullet$, then $(\omega_1\alpha, \omega_2\alpha)$ is a basis of K contained in $\mathfrak{a}$. Hence $\mathfrak{a}$ is a lattice in K. □

The following Definition 5.1.6 is fundamental for the arithmetic of quadratic number fields. It provides the language for the parametrization of quadratic orders by quadratic discriminants in the subsequent Theorem 5.1.7.

Definition 5.1.6. Let Δ be a quadratic discriminant, $K = \mathbb{Q}(\sqrt{\Delta})$ and Δ_K the field discriminant of K. Recall that Δ_K is the fundamental discriminant associated with Δ, it is the unique fundamental discriminant such that $K = \mathbb{Q}(\sqrt{\Delta_K}\,)$, and $\Delta = \Delta_K f_\Delta^2$ (see Theorem 1.1.9 and the remarks preceding and following Theorem 1.1.6). The basis number ω_Δ associated with Δ was defined by

$$\omega_\Delta = \frac{\sigma_\Delta + \sqrt{\Delta}}{2}\,, \qquad \text{where} \quad \sigma_\Delta = \begin{cases} 0 & \text{if} \quad \Delta \equiv 0 \mod 4\,, \\ 1 & \text{if} \quad \Delta \equiv 1 \mod 4\,. \end{cases}$$

Then $\Delta = 4D + \sigma_\Delta$, where $D \in \mathbb{Z}$, and $\omega_\Delta^2 = D + \sigma_\Delta\omega_\Delta \in [1, \omega_\Delta]$. Hence the lattice

$$\mathcal{O}_\Delta = [1, \omega_\Delta] = \mathbb{Z}[\omega_\Delta]$$

is an order in K. It is called the *quadratic order of discriminant* Δ.

Since $(1, \omega_\Delta)$ is linearly independent, it follows that $\mathcal{O}_\Delta \cap \mathbb{Q} = \mathbb{Z}$, and since $\omega_\Delta' = 1 - \omega_\Delta \in \mathcal{O}_\Delta$, we obtain $\mathcal{O}_\Delta' = \mathcal{O}_\Delta$.

The quadratic order $\mathcal{O}_K = \mathcal{O}_{\Delta_K}$ of discriminant Δ_K is called the *maximal order* or the *ring of integers* of K. Indeed, in the subsequent Theorem 5.1.7.3 we shall prove that every order in K is contained in $\mathcal{O}_K$, and afterwards in Theorem 5.1.9 we shall prove that $\mathcal{O}_K = \overline{\mathbb{Z}} \cap K$ consists of all algebraic integers lying in K.

Theorem 5.1.7. *Let Δ be a quadratic discriminant and $K = \mathbb{Q}(\sqrt{\Delta})$. Then*

$$\mathcal{O}_\Delta = \Big\{ \frac{u + v\sqrt{\Delta}}{2} \;\Big|\; u,\, v \in \mathbb{Z}\,,\ u \equiv v\Delta \mod 2 \Big\}\,,$$

and the following assertions hold:

1. *If $f \in \mathbb{N}$, then $\mathcal{O}_{\Delta f^2} = [1, f\omega_\Delta] = \mathbb{Z} + f\mathcal{O}_\Delta \subset \mathcal{O}_\Delta$, and $(\mathcal{O}_\Delta : \mathcal{O}_{\Delta f^2}) = f$. In particular, $\mathcal{O}_\Delta \subset \mathcal{O}_K$, $(\mathcal{O}_K : \mathcal{O}_\Delta) = f_\Delta$, and $\Delta = \Delta_K f_\Delta^2$.*
2. *Let Δ_1 be a quadratic discriminant. Then $\mathcal{O}_{\Delta_1} \subset \mathcal{O}_\Delta$ holds if and only if $\Delta_1 = \Delta f^2$ for some $f \in \mathbb{N}$, and then $f = (\mathcal{O}_\Delta : \mathcal{O}_{\Delta_1})$. In particular, $\mathcal{O}_\Delta = \mathcal{O}_{\Delta_1}$ holds if and only if $\Delta = \Delta_1$.*
3. *$\mathcal{O}_\Delta \subset \mathcal{O}_K$, and $f_\Delta = (\mathcal{O}_K : \mathcal{O}_\Delta)$ is the conductor of Δ.*

Proof. If $u,\, v \in \mathbb{Z}$ and $u \equiv v\Delta \mod 2$, then $u \equiv v\sigma_\Delta \mod 2$, and

$$\frac{u + v\sqrt{\Delta}}{2} = \frac{u - v\sigma_\Delta}{2} + v\omega_\Delta \in [1, \omega_\Delta] = \mathcal{O}_\Delta\,.$$

Conversely, if $\alpha = a + b\omega_\Delta \in \mathcal{O}_\Delta$, where $a,\, b \in \mathbb{Z}$, then

$$\alpha = \frac{(2a + b\sigma_\Delta) + b\sqrt{\Delta}}{2} \quad \text{and} \quad 2a + b\sigma_\Delta \equiv b\Delta \mod 2\,.$$

Hence it follows that

$$\mathcal{O}_\Delta = \Bigl\{ \frac{u + v\sqrt{\Delta}}{2} \;\Bigm|\; u,\, v \in \mathbb{Z}\,,\; u \equiv v\Delta \mod 2 \Bigr\}\,.$$

1. Let $f \in \mathbb{N}$. The identities

$$\omega_{\Delta f^2} = \frac{\sqrt{\Delta f^2}}{2} = f\omega_\Delta \quad \text{if} \quad \Delta \equiv 0 \mod 4\,,$$

$$\omega_{\Delta f^2} = \frac{\sqrt{\Delta f^2}}{2} = -\frac{f}{2} + f\omega_\Delta \quad \text{if} \quad \Delta \equiv 1 \mod 4 \;\; \text{and} \;\; f \equiv 0 \mod 2\,,$$

and

$$\omega_{\Delta f^2} = \frac{1 + \sqrt{\Delta f^2}}{2} = \frac{1 - f}{2} + f\omega_\Delta \quad \text{if} \quad \Delta \equiv 1 \mod 4 \;\; \text{and} \;\; f \equiv 1 \mod 2$$

show that $\mathcal{O}_{\Delta f^2} = [1, \omega_{\Delta f^2}] = [1, f\omega_\Delta] \subset \mathcal{O}_\Delta$. Now

$$\begin{pmatrix} 1 \\ f\omega_\Delta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & f \end{pmatrix} \begin{pmatrix} 1 \\ \omega_\Delta \end{pmatrix} \quad \text{implies} \quad (\mathcal{O}_\Delta : \mathcal{O}_{\Delta f^2}) = \bigl([1, \omega_\Delta] : [1, f\omega_\Delta]\bigr) = f\,.$$

Hence we get $f\mathcal{O}_\Delta \subset \mathcal{O}_{\Delta f^2}$, and therefore $\mathbb{Z} + f\mathcal{O}_\Delta \subset \mathcal{O}_{\Delta f^2}$. On the other hand, $\mathcal{O}_{\Delta f^2} = \mathbb{Z} + \mathbb{Z}f\omega_\Delta \subset \mathbb{Z} + f\mathcal{O}_\Delta$, and thus equality holds. In particular, since Δ_K is the fundamental discriminant associated with Δ, it follows that $\Delta = \Delta_K f_\Delta^2$ and $\mathcal{O}_\Delta \subset \mathcal{O}_{\Delta_K} = \mathcal{O}_K$.

2. If $\Delta_1 = \Delta f^2$, then $\mathcal{O}_{\Delta_1} \subset \mathcal{O}_\Delta$ by 2. Conversely, assume that $\mathcal{O}_{\Delta_1} \subset \mathcal{O}_\Delta$ and $f = (\mathcal{O}_\Delta : \mathcal{O}_{\Delta_1})$. Then $\mathsf{q}(\mathcal{O}_{\Delta_1}) = K$, and $f_{\Delta_1} = (\mathcal{O}_K : \mathcal{O}_{\Delta_1}) = (\mathcal{O}_K : \mathcal{O}_\Delta)\, f = f_\Delta f$. Hence we obtain $\Delta_1 = \Delta_K f_{\Delta_1}^2 = \Delta_K f_\Delta^2 f^2 = \Delta f^2$.

3. By 2., since $\Delta = \Delta_K f_\Delta^2$. □

Let $\Delta \equiv 1 \mod 4$ be a discriminant. An element $\alpha \in \mathcal{O}_\Delta$ is said to have *half-integral coordinates* if

$$\alpha = \frac{u + v\sqrt{\Delta}}{2}\,, \quad \text{where} \quad u,\, v \in \mathbb{Z} \;\; \text{and} \;\; u \equiv v \equiv 1 \mod 2\,.$$

Then $\mathcal{O}_\Delta \setminus \mathcal{O}_{4\Delta}$ is the set of all $\alpha \in \mathcal{O}_\Delta$ having half-integral coordinates.

Exercise 5.1.8. Let Δ be a quadratic discriminant.

a) Prove that

$$\mathcal{O}_\Delta = \Bigl[1, \frac{\Delta + \sqrt{\Delta}}{2}\Bigr]\,, \quad \text{and} \quad \partial(\mathcal{O}_\Delta) = \Delta\,,$$

where $\partial(\mathcal{O}_\Delta)$ is defined in Exercise 5.1.4.

b) For $f \in \mathbb{N}$, prove that

$$\mathcal{O}_{\Delta f^2} = \Bigl\{ \frac{a + b\sqrt{\Delta}}{2} \;\Bigm|\; a \equiv b\Delta \mod 2 \;\; \text{and} \;\; b \equiv 0 \mod f \Bigr\}\,,$$

and if $f = \operatorname{lcm}(f_1, f_2)$ for some $f_1,\, f_2 \in \mathbb{N}$, then $\mathcal{O}_{\Delta f^2} = \mathcal{O}_{\Delta f_1^2} \cap \mathcal{O}_{\Delta f_2^2}$.

The following theorem justifies the name “ring of integers” for the maximal order of a quadratic number field and proves that it is integrally closed (see Theorem A.9.3).

Theorem 5.1.9. *Let K be a quadratic number field. For $\xi \in K$, the following assertions are equivalent*:

(a) $\xi \in \mathcal{O}_K$.

(b) *ξ is an algebraic integer.*

(c) $\mathcal{N}(\xi) \in \mathbb{Z}$ *and* $\mathcal{T}(\xi) \in \mathbb{Z}$.

(d) *Either $\xi \in \mathbb{Z}$, or ξ is a quadratic irrational of type (a,b,c) such that $|a| = 1$.*

(e) *There exists a lattice $\mathfrak{a}$ in K such that $\xi\mathfrak{a} \subset \mathfrak{a}$.*

In particular, $\mathcal{O}_K = \overline{\mathbb{Z}} \cap K$ is integrally closed.

Proof. (a) $\Rightarrow$ (b) If $\xi \in \mathcal{O}_K$, then

$$\xi = \frac{a + b\sqrt{\Delta_K}}{2}, \quad \text{where} \quad a,\, b \in \mathbb{Z} \ \text{ and } \ a \equiv b\Delta_K \bmod 2\,,$$

hence $a^2 - b^2\Delta_K \equiv 0 \bmod 4$, and therefore

$$\xi^2 - a\xi + \frac{a^2 - b^2\Delta_K}{4} = 0$$

is an integral equation for ξ, which proves that ξ is an algebraic integer.

(b) $\Rightarrow$ (c) If $\xi^n + a_{n-1}\xi^{n-1} + \ldots + a_1\xi + a_0 = 0$ is an integral equation for ξ (where $n \in \mathbb{N}$ and $a_0, \ldots, a_{n-1} \in \mathbb{Z}$), then $\xi'^n + a_{n-1}\xi'^{n-1} + \ldots + a_1\xi' + a_0 = 0$. Hence ξ' is also an algebraic integer, and as $\xi,\, \xi' \in \overline{\mathbb{Z}}$, it follows that $\mathcal{N}(\xi) = \xi\xi' \in \overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$ and $\mathcal{T}(\xi) = \xi + \xi' \in \overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$ (see Corollary A.9.4).

(c) $\Rightarrow$ (d) Suppose that $\xi \notin \mathbb{Z}$, and observe that $\xi^2 - \mathcal{T}(\xi)\xi + \mathcal{N}(\xi) = 0$. If (a,b,c) is the type of ξ, then Theorem 1.1.2.2, implies that there is some $y \in \mathbb{Z}$ such that $1 = ay$ and thus $|a| = 1$.

(d) $\Rightarrow$ (a) If $\xi \in \mathbb{Z}$, there is nothing to do. Thus let ξ be a quadratic irrational of type (a,b,c) and discriminant Δ such that $|a| = 1$. Then $\Delta = b^2 - 4ac = \Delta_K f^2$ for some $f \in \mathbb{N}$, hence $b \equiv f\Delta_K \bmod 2$, and therefore

$$\xi = \frac{b + \sqrt{\Delta}}{2a} = \frac{ab + af\sqrt{\Delta_K}}{2} \in \mathcal{O}_K\,.$$

(a) $\Rightarrow$ (e) Set $\mathfrak{a} = \mathcal{O}_K$.

(e) $\Rightarrow$ (b) Let $\mathfrak{a} = [\omega_1, \omega_2]$ be a lattice in K such that $\xi\mathfrak{a} \subset \mathfrak{a}$. Then

$$\xi \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = A \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} \qquad \text{for some matrix } A \in \mathsf{M}_2(\mathbb{Z}).$$

Hence ξ is a zero of the characteristic polynomial of A, which is an integral equation for ξ.

The equivalence of (a) and (b) implies that $\mathcal{O}_K = K \cap \overline{\mathbb{Z}}$ is integrally closed. $\square$

Exercise 5.1.10. Let Δ be a quadratic discriminant, $\alpha \in \mathcal{O}_\Delta$ and $a \in \mathbb{Z}$. Prove the equivalence of the following conditions (consult Section A.8 if necessary) :

a) $(\alpha, a) = 1$; **b)** $(\alpha', a) = 1$ **c)** $(\mathcal{N}(\alpha), a) = 1$.

Exercise 5.1.11. Let K be a quadratic number field, $\xi \in K$, and suppose that ξ satisfies an equation of the form $\xi^n + \alpha_{n-1}\xi^{n-1} + \ldots + \alpha_1\xi + \alpha_0$ for some $n \in \mathbb{N}$ and $\alpha_0, \ldots, \alpha_{n-1} \in \mathcal{O}_K$. Prove that $\xi \in \mathcal{O}_K$. Hint: Mimic the proof of Theorem A.9.1.

Theorem 5.1.12. *Let K be a quadratic number field and $R \subset K$. Then the following assertions are equivalent*:

(a) *R is an order in K.*

(b) *There is some lattice $\mathfrak{a}$ in K such that $R = \mathcal{R}(\mathfrak{a})$.*

(c) *R is a subring of O_K, and for every $z \in K$ there is some $m \in \mathbb{N}$ such that $mz \in R$.*

(d) *$R = \mathcal{O}_\Delta$ for some quadratic discriminant Δ.*

Proof. (a) $\Rightarrow$ (b) Set $\mathfrak{a} = R$.

(b) $\Rightarrow$ (c) Let $\mathfrak{a}$ be a lattice in K such that $R = \mathcal{R}(\mathfrak{a})$. By Theorem 5.1.5.1, R is an order in K. In particular, R is a subring of K, and for every $z \in K$ there is some $m \in \mathbb{N}$ such that $mz \in R$. If $\xi \in R$, then $\xi\mathfrak{a} \subset \mathfrak{a}$, and Theorem 5.1.9 implies that $\xi \in \mathcal{O}_K$. Hence it follows that $R \subset \mathcal{O}_K$.

(c) $\Rightarrow$ (d) By assumption, R is a lattice in K, $f = (\mathcal{O}_K : R) < \infty$ (see Theorem A.4.2.4), and therefore $f\omega_{\Delta_K} \in R$. It follows that $\mathcal{O}_{\Delta_K f^2} = [1, f\omega_{\Delta_K}] \subset R$, and since $(\mathcal{O}_K : \mathcal{O}_{\Delta_K f^2}) = f = (\mathcal{O}_K : R)$, we obtain $R = \mathcal{O}_{\Delta_K f^2}$.

(d) $\Rightarrow$ (a) Obvious. □

Corollary 5.1.13. *If K is a quadratic number field and $\mathfrak{a}$ is a lattice in K, then $\mathcal{R}(\mathfrak{a}') = \mathcal{R}(\mathfrak{a})' = \mathcal{R}(\mathfrak{a})$.*

Proof. By Theorem 5.1.12, $\mathcal{R}(\mathfrak{a}) = \mathcal{O}_\Delta$ for some quadratic discriminant Δ. Since $\alpha \mapsto \alpha'$ is an automorphism, we obtain $\mathcal{R}(\mathfrak{a}') = \mathcal{R}(\mathfrak{a})' = \mathcal{O}_\Delta' = \mathcal{O}_\Delta$. □

5.2. Units in quadratic orders

In this section, we determine the algebraic structure of the unit group $\mathcal{O}_\Delta^\times$ of a quadratic order $\mathcal{O}_\Delta$ and investigate the connection with Pell's equation. Note that we already met Pell's equation several times in this volume (namely in the remarks after Theorem 1.2.2, in Theorem 1.2.3 and in Theorem 2.2.9).

In a first theorem we shall connect the invertible elements of a quadratic order with the solutions of Pell's equation, and then we shall apply our knowledge of these solutions to disclose the algebraic structure of the unit group of a quadratic order.

Theorem 5.2.1 (Unit theorem for quadratic orders). *Let Δ be a quadratic discriminant. Then the unit group $\mathcal{O}_\Delta^\times$ of $\mathcal{O}_\Delta$ is given by*

$$\mathcal{O}_\Delta^\times = \{\xi \in \mathcal{O}_\Delta \mid \mathcal{N}(\xi) = \pm 1\} = \Big\{\frac{u + v\sqrt{\Delta}}{2} \;\Big|\; u,\, v \in \mathbb{Z}\,,\ |u^2 - \Delta v^2| = 4\Big\}\,.$$

The group $\mathbb{W}(\mathcal{O}_\Delta)$ of roots of unity in $\mathcal{O}_\Delta$ is a finite subgroup of $\mathcal{O}_\Delta^\times$, given by

$$\mathbb{W}(\mathcal{O}_\Delta) = \begin{cases} \langle \mathsf{i} \rangle & \text{if } \ \Delta = -4\,, \\ \langle -\zeta_3 \rangle & \text{if } \ \Delta = -3\,, \\ \langle -1 \rangle & \text{otherwise}\,, \end{cases} \quad \text{and} \quad |\mathbb{W}(\mathcal{O}_\Delta)| = \begin{cases} 4 & \text{if } \ \Delta = -4\,, \\ 6 & \text{if } \ \Delta = -3\,, \\ 2 & \text{otherwise}\,. \end{cases}$$

1. *If $\Delta < 0$, then $\mathcal{O}_\Delta^\times = \mathbb{W}(\mathcal{O}_\Delta)$.*
2. *Suppose that $\Delta > 0$.*
   (a) *If*

$$\varepsilon = \frac{u + v\sqrt{\Delta}}{2} \in \mathcal{O}_\Delta^\times\,, \quad \text{where} \quad u,\, v \in \mathbb{Z} \ \text{ and } u \equiv v \mod 2\,,$$

then $\varepsilon > 1$ if and only if $u > 0$ and $v > 0$.

   (b) *If ε_Δ denotes the fundamental unit of discriminant Δ (as introduced in* Theorem 2.2.9 *), then $\mathcal{O}_\Delta^\times = \langle -1,\, \varepsilon_\Delta \rangle$. In particular, $\mathcal{O}_\Delta^\times$ is an infinite group, $\mathcal{O}_\Delta^\times \cap \mathbb{R}_{>0} = \langle \varepsilon_\Delta \rangle$, and*

$$\varepsilon_\Delta = \min\{\varepsilon \in \mathcal{O}_\Delta^\times \mid \varepsilon > 1\} = \frac{u + v\sqrt{\Delta}}{2} \quad \text{for some} \quad u,\, v \in \mathbb{N}\,.$$

Proof. If $\xi \in \mathcal{O}_\Delta^\times$, then $\{\xi, \xi^{-1}\} \subset \mathcal{O}_\Delta$ implies $\{\mathcal{N}(\xi),\, \mathcal{N}(\xi^{-1})\} \subset \mathbb{Z}$, and since $1 = \mathcal{N}(\xi\xi^{-1}) = \mathcal{N}(\xi)\mathcal{N}(\xi^{-1})$, it follows that $\mathcal{N}(\xi) \in \{\pm 1\}$. Conversely, if $\xi \in \mathcal{O}_\Delta$ and $\mathcal{N}(\xi) = \pm 1$, then $\xi' \in \mathcal{O}_\Delta$, and $\mathcal{N}(\xi) = \xi\xi' = \pm 1$ implies $\xi \in \mathcal{O}_\Delta^\times$. Thus we have proved that $\mathcal{O}_\Delta^\times = \{\xi \in \mathcal{O}_\Delta \mid \mathcal{N}(\xi) = \pm 1\}$.

If $\xi \in \mathcal{O}_\Delta$, then there exist $u,\, v \in \mathbb{Z}$ such that

$$u \equiv v\Delta \mod 2\,, \quad \xi = \frac{u + v\sqrt{\Delta}}{2}\,, \quad \text{and} \quad \mathcal{N}(\xi) = \frac{u^2 - v^2\Delta}{4}\,.$$

Hence it follows that $\mathcal{N}(\xi) = \pm 1$ if and only if $u^2 - \Delta v^2 = \pm 4$. Since $u^2 - \Delta v^2 = \pm 4$ implies $u \equiv v\Delta \mod 2$, this latter condition can be omitted.

1. Obviously, $\mathbb{W}(\mathcal{O}_\Delta)$ is a subgroup of $\mathcal{O}_\Delta^\times$. If $\Delta > 0$, then $\mathcal{O}_\Delta \subset \mathbb{R}$, and therefore $\mathbb{W}(\mathcal{O}_\Delta) = \{\pm 1\}$. If $\Delta < 0$, we refer to the (simple) calculations made after Theorem 1.2.2 : There it was shown that

$$\Big\{\frac{u + v\sqrt{\Delta}}{2} \;\Big|\; u^2 - \Delta v^2 = \pm 4\Big\} = \Big\{\frac{u + v\sqrt{\Delta}}{2} \;\Big|\; u^2 - \Delta v^2 = \Big\} = \begin{cases} \mathbb{W}_2 & \text{if } \ \Delta < -4\,, \\ \mathbb{W}_6 & \text{if } \ \Delta = -3\,, \\ \mathbb{W}_4 & \text{if } \ \Delta = -4\,. \end{cases}$$

2. (a) Assume that $\Delta > 0$, and

$$\varepsilon = \frac{u + v\sqrt{\Delta}}{2} \in \mathcal{O}_\Delta^\times \setminus \{\pm 1\}\,, \quad \text{where} \quad u,\, v \in \mathbb{Z} \ \text{ and } \ u \equiv v\Delta \mod 2\,.$$

Then there is a unique $\overline{\varepsilon} \in \{\pm\varepsilon,\, \pm\varepsilon^{-1}\}$ such that $\overline{\varepsilon} > 1$, namely

$$\overline{\varepsilon} = \max\{\pm\varepsilon,\, \pm\varepsilon^{-1}\} = \max\Bigl\{\frac{\sigma u + \tau v\sqrt{\Delta}}{2} \Bigm| \sigma,\, \tau \in \{\pm 1\}\Bigr\} = \frac{|u| + |v|\sqrt{\Delta}}{2}\,.$$

Hence it follows that $\varepsilon > 1$ if and only if $u > 0$ and $v > 0$.

(b) Let ε_Δ be the fundamental unit of discriminant Δ. We proved in Theorem 2.2.9 that there exist $u,\, v \in \mathbb{N}$ such that

$$\varepsilon_\Delta = \frac{u + v\sqrt{\Delta}}{2} > 1\,,$$

and that

$$\mathcal{O}_\Delta^\times = \Bigl\{\frac{u + v\sqrt{\Delta}}{2} \Bigm| u,\, v \in \mathbb{Z}\,,\ |u^2 - \Delta v^2| = 4\Bigr\} = \langle -1, \varepsilon_\Delta\rangle\,.$$

Hence it follows that $\mathcal{O}_\Delta^\times \cap \mathbb{R}_{>0} = \langle \varepsilon_\Delta\rangle$, and $\varepsilon_\Delta = \min\{\varepsilon \in \mathcal{O}_\Delta^\times \mid \varepsilon > 1\,\}$. □

The above proof of the unit theorem for positive discriminants, though very short, is unsatisfactory inasmuch as it relies on the existence of ε_Δ proved using the theory of continued fractions. We shall now give a second proof which only uses simple geometric ideas together with the fact that Pell's equation $x^2 - dy^2 = 1$ for $d \in \mathbb{N}$ has infinitely many solutions (note that we gave an elementary proof of this fact in Theorem 1.2.3).

A SECOND PROOF OF THE UNIT THEOREM FOR POSITIVE DISCRIMINANTS. Let $\Delta > 0$ be a quadratic discriminant. Suppose that we already know that Pell's equation $x^2 - \Delta y^2 = 1$ has infinitely many solutions and that

$$\mathcal{O}_\Delta^\times = \Bigl\{\frac{u + v\sqrt{\Delta}}{2} \Bigm| u,\, v \in \mathbb{Z}\,,\ |u^2 - \Delta v^2| = 4\Bigr\}.$$

Then $\mathcal{O}_\Delta^\times$ is an infinite subgroup of $\mathbb{R}^\times$, and we shall prove that $\mathcal{O}_\Delta^\times = \langle -1, \varepsilon_0\rangle$, where

$$\varepsilon_0 = \min(\mathcal{O}_\Delta^\times \cap \mathbb{R}_{>1}) = \frac{u_0 + v_0\sqrt{\Delta}}{2} \quad \text{for some} \quad u_0,\, v_0 \in \mathbb{N}\,.$$

For $\varepsilon \in \mathcal{O}_\Delta^\times \setminus \{\pm 1\}$, we define $\varepsilon^* = \max\{\pm\varepsilon, \pm\varepsilon^{-1}\} \in \mathcal{O}_\Delta^\times \cap \mathbb{R}_{>1}$. If $u,\, v \in \mathbb{Z}$, then

$$\varepsilon = \frac{u + v\sqrt{\Delta}}{2} \quad \text{implies} \quad \{\pm\varepsilon, \pm\varepsilon^{-1}\} = \Bigl\{\frac{\sigma u + \tau v\sqrt{\Delta}}{2} \Bigm| \sigma,\, \tau \in \{\pm 1\}\Bigr\},$$

and therefore

$$\varepsilon^* = \frac{|u| + |v|\sqrt{\Delta}}{2} \ge \frac{1 + \sqrt{\Delta}}{2}\,.$$

Hence it follows that $\varepsilon_0 = \inf(\mathcal{O}_\Delta^\times \cap \mathbb{R}_{>1}) > 1$, and we assert that $\varepsilon_0 \in \mathcal{O}_\Delta^\times$. Indeed, otherwise there exists a monotonically decreasing sequence $(\varepsilon_n)_{n\ge 1}$ in $\mathcal{O}_\Delta^\times \cap \mathbb{R}_{>1}$ which converges to ε_0, and then it follows that

$$\frac{\varepsilon_n}{\varepsilon_{n+1}} \in \mathcal{O}_\Delta^\times \cap \mathbb{R}_{>1} \ \text{ for all } \ n \in \mathbb{N}\,, \quad \text{and} \quad \lim_{n\to\infty} \frac{\varepsilon_n}{\varepsilon_{n+1}} = 1\,,$$

a contradiction. Since $\varepsilon_0 > 1$, it follows that $\varepsilon_0 = \varepsilon_0^*$, and therefore

$$\varepsilon_0 = \frac{u_0 + v_0\sqrt{\Delta}}{2}\,, \quad \text{where} \quad u_0,\, v_0 \in \mathbb{N}\,.$$

Clearly, $\varepsilon_0 \in \mathcal{O}_\Delta^\times$ implies $\langle -1, \varepsilon_0\rangle \subset \mathcal{O}_\Delta^\times$. To prove the reverse inclusion, suppose that $\varepsilon \in \mathcal{O}_\Delta^\times \setminus \{\pm 1\}$, and let $k \in \mathbb{N}$ be maximal such that $\varepsilon_0^k \le \varepsilon^*$. Then $\varepsilon^* < \varepsilon_0^{k+1}$, hence $1 \le \varepsilon^*\varepsilon_0^{-k} < \varepsilon_0$, and since $\varepsilon^*\varepsilon_0^{-k} \in \mathcal{O}_\Delta^\times$, it follows that $\varepsilon^* = \varepsilon_0^k$, and therefore $\varepsilon \in \{\pm\varepsilon^*, \pm(\varepsilon^*)^{-1}\} \subset \langle -1, \varepsilon_0\rangle$. □

Besides the unit group $\mathcal{O}_\Delta^\times$, we consider its subgroup

$$\mathcal{O}_\Delta^{\times +} = \{\xi \in \mathcal{O}_\Delta \mid \mathcal{N}(\xi) = 1\} = \Big\{\frac{u + v\sqrt{\Delta}}{2} \;\Big|\; u,\, v \in \mathbb{Z}\,,\; u^2 - \Delta v^2 = 4\Big\}$$

of norm-positive units. Note that $\mathcal{O}_\Delta^{\times +} = \{\xi \in \mathcal{O}_\Delta^\times \mid \mathcal{N}(\xi) > 0\}$, and if $\Delta < 0$, then $\mathcal{O}_\Delta^\times = \mathcal{O}_\Delta^{\times +}$. If $\Delta > 0$, then

$$\mathcal{O}_\Delta^{\times +} = \langle -1, \varepsilon_\Delta^+\rangle\,, \quad \text{where} \quad \varepsilon_\Delta^+ = \begin{cases} \varepsilon_\Delta & \text{if} \quad \mathcal{N}(\varepsilon_\Delta) = 1\,, \\ \varepsilon_\Delta^2 & \text{if} \quad \mathcal{N}(\varepsilon_\Delta) = -1\,, \end{cases}$$

and we call ε_Δ^+ the *norm-positive fundamental unit* of discriminant Δ. It follows that $\mathcal{O}_\Delta^\times = \mathcal{O}_\Delta^{\times +}$ if and only if Pell's minus equation has no integral solutions, and $(\mathcal{O}_\Delta^\times : \mathcal{O}_\Delta^{\times +}) = 2$ otherwise.

By definition, $\mathcal{N}(\varepsilon_\Delta) = -1$ holds if and only if Pell's minus equation has integral solutions, and by Theorem 2.3.5, this is true if and only if the period length $l(\omega_\Delta)$ of the continued fraction of ω_Δ is odd.

It is a delicate problem and beyond the scope of this volume to determine necessary and sufficient conditions (not depending on continued fractions) for the solubility of Pell's minus equation (see [**81**] and the papers by L. Redei cited there). We proceed with a simple necessary criterion.

Theorem 5.2.2. *Let $\Delta > 0$ be a quadratic discriminant, and suppose that $\mathcal{N}(\varepsilon_\Delta) = -1$. Then Δ has no prime factor $p \equiv 3 \mod 4$.*

Proof. Let p be an odd prime dividing Δ, and suppose that there exist $u,\, v \in \mathbb{Z}$ such that $u^2 - v^2\Delta = -4$. Then $u^2 \equiv -4 \mod p$, hence

$$1 = \Big(\frac{-4}{p}\Big) = \Big(\frac{-1}{p}\Big)\,, \quad \text{and therefore} \quad p \equiv 1 \mod 4\,.$$ □

The criterion of Theorem 5.2.2 is not sufficient. For example, $\varepsilon_{34} = 35 + 6\sqrt{34}$ and $\mathcal{N}(\varepsilon_{34}) = 1$. In Theorem 5.6.13 we shall prove that $\mathcal{N}(\varepsilon_\Delta) = -1$ if $\Delta = p^r$ or $\Delta = 4p^r$ for some prime $p \equiv 1 \mod 4$ and an odd exponent $r \in \mathbb{N}$.

We proceed with a comparison of the unit groups of $\mathcal{O}_\Delta$ and $\mathcal{O}_{\Delta f^2}$ for some integer $f \ge 2$. If $\Delta < 0$, it is plain by Theorem 5.2.1 that

$$(\mathcal{O}_\Delta^\times : \mathcal{O}_{\Delta f^2}^\times) = \frac{|\mathbb{W}(\mathcal{O}_\Delta)|}{|\mathbb{W}(\mathcal{O}_{\Delta f^2})|} = \begin{cases} 3 & \text{if} \quad \Delta = -3\,, \\ 2 & \text{if} \quad \Delta = -4\,, \\ 1 & \text{otherwise}\,. \end{cases}$$

To investigate the situation for $\Delta > 0$ we must revert to the theory of continued fractions.

Theorem 5.2.3. *Let $\Delta > 0$ be a quadratic discriminant.*

1. *Suppose that $\Delta \equiv 1 \bmod 4$ and ε_Δ has half-integral coordinates. Then it follows that $\{\varepsilon_\Delta, \varepsilon_\Delta^2\} \subset \mathcal{O}_\Delta^\times \setminus \mathcal{O}_{4\Delta}$, $\Delta \equiv 5 \bmod 8$, $\varepsilon_\Delta^3 = \varepsilon_{4\Delta} \in \mathbb{Z}[\sqrt{\Delta}] = \mathcal{O}_{4\Delta}$, and $(\mathcal{O}_\Delta^\times : \mathcal{O}_{4\Delta}^\times) = 3$.*
2. *Let $f \geq 2$ be an integer. Then $\mathcal{O}_{\Delta f^2}^\times = \mathcal{O}_{\Delta f^2} \cap \mathcal{O}_\Delta^\times$,*
$$d = (\mathcal{O}_\Delta^\times : \mathcal{O}_{\Delta f^2}^\times) = \min\{n \in \mathbb{N} \mid \varepsilon_\Delta^n \in \mathcal{O}_{\Delta f^2}\} < \infty\,, \quad \textit{and} \quad \varepsilon_{\Delta f^2} = \varepsilon_\Delta^d\,.$$
If $l = l(\omega_\Delta)$ is the period length and $(q_n)_{n \geq -2}$ is the sequence of partial denominators of ω_Δ, then $d\mathbb{N} = \{n \in \mathbb{N} \mid q_{nl-1} \equiv 0 \bmod f\}$.

Proof. 1. Let $u,\, v \in \mathbb{Z}$ be such that $u \equiv v \equiv 1 \bmod 2$,
$$\varepsilon_\Delta = \frac{u + v\sqrt{\Delta}}{2} \quad \text{and} \quad \varepsilon_\Delta^3 = \frac{(u^2 + 3v^2\Delta) + v(3u^2 + v^2\Delta)\sqrt{\Delta}}{8}\,.$$
Since $|u^2 - v^2\Delta| = 4$, we obtain $4 \equiv u^2 - v^2\Delta \equiv 1 - \Delta \bmod 8$, hence $\Delta \equiv 5 \bmod 8$ and $u^2 + 3v^2\Delta \equiv 3u^2 + v^2\Delta \equiv 0 \bmod 8$. It follows that $\varepsilon_\Delta^3 \in \mathcal{O}_{4\Delta}^\times$, and as $\varepsilon_\Delta \notin \mathcal{O}_{4\Delta}^\times$, we obtain $(\mathcal{O}_\Delta^\times : \mathcal{O}_{4\Delta}^\times) = 3$, $\varepsilon_\Delta^2 \notin \mathcal{O}_{4\Delta}^\times$, and $\varepsilon_\Delta^3 = \varepsilon_{4\Delta} \in \mathcal{O}_{4\Delta} = \mathbb{Z}[\sqrt{\Delta}\,]$.

2. Obviously, $\mathcal{O}_\Delta^\times \cap \mathcal{O}_{\Delta f^2} = \{\xi \in \mathcal{O}_{\Delta f^2} \mid \mathcal{N}(\xi) = \pm 1\} = \mathcal{O}_{\Delta f^2}^\times$, and $\mathcal{O}_{\Delta f^2}^\times \cap \mathbb{R}_{>0}$ is a subgroup of $\mathcal{O}_\Delta^\times \cap \mathbb{R}_{>0} = \langle \varepsilon_\Delta \rangle$. If $d \in \mathbb{N}$ is minimal such that $\varepsilon_\Delta^d \in \mathcal{O}_{\Delta f^2}$ (and thus $\varepsilon_\Delta^d \in \mathcal{O}_{\Delta f^2} \cap \mathbb{R}_{>0}$), then $\mathcal{O}_{\Delta f^2}^\times \cap \mathbb{R}_{>0} = \langle \varepsilon^d \rangle$. Hence it follows that $\varepsilon_\Delta^d = \varepsilon_{\Delta f^2}$, and $(\mathcal{O}_\Delta^\times : \mathcal{O}_{\Delta f^2}^\times) = (\langle -1, \varepsilon_\Delta \rangle : \langle -1, \varepsilon_\Delta^d \rangle) = d$.

If $(p_n)_{n \geq -2}$ denotes the sequence of partial numerators of ω_Δ, then Theorem 2.3.5.4 implies $\varepsilon_\Delta^n = p_{nl-1} - q_{nl-1}\omega_\Delta'$ for all $n \in \mathbb{N}_0$. Since $\mathcal{O}_{\Delta f^2} = \mathbb{Z} + \mathbb{Z}f\omega_\Delta'$ and $\mathcal{O}_{\Delta f^2}^\times = \mathcal{O}_\Delta^\times \cap \mathcal{O}_{\Delta f^2}$, it follows that $\omega_\Delta^n \in \mathcal{O}_{\Delta f^2}^\times$ if and only if $q_{nl-1} \equiv 0 \bmod f$, and therefore $\{n \in \mathbb{N} \mid q_{nl-1} \equiv 0 \bmod f\} = \{n \in \mathbb{N} \mid \varepsilon_\Delta^n \in \mathcal{O}_{\Delta f^2}^\times\} = d\mathbb{N}$. □

Exercise 5.2.4. Let $\Delta > 0$ be a quadratic discriminant such that $\mathcal{N}(\varepsilon_\Delta) = -1$.

a) Suppose that $f = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$, where $r \in \mathbb{N}$, $e_1, \ldots, e_r \in \mathbb{N}$ and $p_1, \ldots, p_r$ are distinct primes. Prove that the following conditions are equivalent:

- There is some odd $k \in \mathbb{N}$ such that $\varepsilon_\Delta^{2k} + 1 \in f\mathcal{O}_\Delta$.
- $\mathcal{N}(\varepsilon_{\Delta f^2}) = -1$.
- $\mathcal{N}(\varepsilon_{\Delta p_i^2}) = -1$ for all $i \in [1, r]$.

b) Let $p = 1 + 2^\lambda u$ be a prime, where $\lambda \in \mathbb{N}_{\geq 2}$ and $u \in \mathbb{N}$ is odd. Suppose that Δ is a quadratic residue modulo p, and let $d \in \mathbb{Z}$ be such that $d^2 \equiv \Delta \bmod 2p$. If $\varepsilon_\Delta = (u + v\sqrt{\Delta})/2$, we set $e_\Delta = (u + vd)/2$ and call e_Δ a rational representative of ε_Δ modulo p. Prove that $\mathcal{N}(\varepsilon_{\Delta p^2}) = -1$ if and only if $e^{2u} \equiv -1 \bmod p$.
(Compare [**46**].)

We apply Theorem 5.2.1 to characterize the structure and the absolute norm of non-zero principal ideals of $\mathcal{O}_\Delta$ (note that $\mathcal{O}_\Delta^\times$ is the set of generators of the unit ideal $\mathcal{O}_\Delta$).

Theorem 5.2.5. *Let $\Delta > 0$ be a quadratic discriminant and $\mathfrak{a}$ a non-zero principal ideal of $\mathcal{O}_\Delta$.*

1. *There exists a unique $\alpha_0 \in \mathcal{O}_\Delta$ such that $1 < \alpha_0 \le \varepsilon_\Delta$ and $\mathfrak{a} = \alpha_0\mathcal{O}_\Delta$, namely $\alpha_0 = \min\{\alpha \in \mathcal{O}_\Delta \mid \alpha > 1,\ \mathfrak{a} = \alpha\mathcal{O}_\Delta\}$, and then*
$$\{\alpha \in \mathcal{O}_\Delta \mid \mathfrak{a} = \alpha\mathcal{O}_\Delta\} = \{\pm\varepsilon_\Delta^m\alpha_0 \mid m \in \mathbb{Z}\}.$$
If we assume that
$$\alpha_0 = \frac{u_0 + v_0\sqrt{\Delta}}{2}, \quad \text{where} \quad u_0,\, v_0 \in \mathbb{N},$$
then it follows that, for all $m \in \mathbb{N}_0$,
$$\varepsilon_\Delta^m\alpha_0 = \frac{u_m + v_m\sqrt{\Delta}}{2}, \quad \text{where} \quad u_m,\, v_m \in \mathbb{N}, \quad u_m \equiv v_m\Delta \mod 2,$$
and if $\Delta > 5$, then the sequences $(u_m)_{m\ge0}$ and $(v_m)_{m\ge0}$ are strictly monotonically increasing.
2. *For $m \in \mathbb{N}$, we have*
$$\varepsilon_\Delta^m = \frac{u_m + v_m\sqrt{\Delta}}{2}, \quad \text{where} \quad u_m,\, v_m \in \mathbb{N}, \quad u_m \equiv v_m\Delta \mod 2,$$
and if $\Delta > 5$, then the sequences $(u_m)_{m\ge0}$ and $(v_m)_{m\ge0}$ are strictly monotonically increasing.
3. *Suppose that $\mathfrak{a} = \alpha_1\mathcal{O}_\Delta$ for some $\alpha_1 \in \mathcal{O}_\Delta$ such that $\mathcal{N}(\alpha_1) > 0$. Then there exists a unique $\alpha_0 \in \mathcal{O}_\Delta$ such that $\alpha_0 > 0$, $\mathcal{N}(\alpha_0) > 0$, $\mathfrak{a} = \alpha_0\mathcal{O}_\Delta$, and*
$$1 < \frac{\alpha_0'}{\alpha_0} \le \varepsilon_\Delta^{+2},$$
where ε_Δ^+ denotes the norm-positive fundamental unit of discriminant Δ.

PROOF. 1. If $\mathfrak{a} = \alpha_1\mathcal{O}_\Delta$, where $\alpha_1 \in \mathcal{O}_\Delta^\bullet$, then
$$\{\alpha \in \mathcal{O}_\Delta \mid \mathfrak{a} = \alpha\mathcal{O}_\Delta\} = \{\eta\alpha_1 \mid \eta \in \mathcal{O}_\Delta^\times\}.$$
By Theorem 5.2.1, we have
$$\mathcal{O}_\Delta^\times = \langle -1, \varepsilon_\Delta\rangle, \quad \text{where} \quad \varepsilon_\Delta = \frac{u + v\sqrt{\Delta}}{2} > 1$$
for some $u,\, v \in \mathbb{N}$ such that $|u^2 - \Delta v^2| = 4$. Hence there exists a unique $\eta \in \mathcal{O}_\Delta^\times$ such that $1 < \alpha_0 = \eta\alpha_1 \le \varepsilon_\Delta$, and then $\alpha_0 = \min\{\alpha \in \mathcal{O}_\Delta \mid \alpha > 1,\ \mathfrak{a} = \alpha\mathcal{O}_\Delta\}$.

Assume now that
$$\alpha_0 = \frac{u_0 + v_0\sqrt{\Delta}}{2}, \quad \text{where} \quad u_0,\, v_0 \in \mathbb{N}.$$
For $m \in \mathbb{N}_0$, we obtain
$$\begin{aligned}\frac{u_{m+1} + v_{m+1}\sqrt{\Delta}}{2} &= \frac{u_m + v_m\sqrt{\Delta}}{2}\,\frac{u + v\sqrt{\Delta}}{2} \\ &= \frac{1}{2}\Big(\frac{u_mu + v_mv\Delta}{2} + \frac{v_mu + u_mv}{2}\sqrt{\Delta}\Big),\end{aligned}$$

and therefore

$$u_{m+1} = \frac{u_m u + v_m v\Delta}{2} \quad \text{and} \quad v_{m+1} = \frac{v_m u + u_m v}{2}\,.$$

A simple induction shows that $u_m,\, v_m \in \mathbb{N}$ for all $m \in \mathbb{N}_0$. If $u \ge 2$, then both sequences are strictly monotonically increasing. However, if $u = 1$, then we obtain $1 = u^2 \ge \Delta v^2 - 4 \ge 5v^2 - 4 \ge 1$ and thus $\Delta = 5$, which is the exceptional case.

2. By 1., applied with $\alpha_0 = \varepsilon_\Delta$.

3. We may assume that $\alpha_1 > 0$ (otherwise we consider $-\alpha_1$), and we observe that

$$\frac{\alpha_1'}{\alpha_1} = \frac{\alpha_1'^2}{\mathcal{N}(\alpha_1)} > 0\,.$$

If ε_Δ^+ denotes the norm-positive fundamental unit of discriminant Δ, then

$$\mathcal{O}_\Delta^{\times +} = \{\eta \in \mathcal{O}_\Delta^\times \mid \mathcal{N}(\eta) = 1\} = \langle -1, \varepsilon_\Delta^+ \rangle\,,$$

and therefore

$$\{\alpha \in \mathcal{O}_\Delta \mid \mathfrak{a} = \alpha\mathcal{O}_\Delta\,,\ \alpha > 0,\ \mathcal{N}(\alpha) > 0\} = \{\varepsilon_\Delta^{+m}\alpha_1 \mid m \in \mathbb{Z}\}\,.$$

The assertion follows since there exists a unique $m \in \mathbb{Z}$ such that $\alpha_0 = \varepsilon_\Delta^{+m}\alpha_1$ satisfies the inequalities

$$1 < \frac{\alpha_0'}{\alpha_0} = \frac{\alpha_1'}{\varepsilon_\Delta^{+2m}\alpha_1} \le \varepsilon_\Delta^{+2}\,. \qquad \square$$

Corollary 5.2.6. *Let $\Delta > 5$ be a quadratic discriminant and $u \in \mathbb{N}$ such that $|u^2 - \Delta| = 4$. Then*

$$\varepsilon_\Delta = \frac{u + \sqrt{\Delta}}{2}\,.$$

Proof. By definition, $\eta = (u + v\sqrt{\Delta}\,)/2 \in \mathcal{O}_\Delta^\times$ and $\eta > 1$. Hence it follows that $\eta = \varepsilon_\Delta^m$ for some $m \in \mathbb{N}$, and Theorem 5.2.5.2 implies $m = 1$. $\square$

Exercise 5.2.7. Discuss the exceptional case $\Delta = 5$ of Theorem 5.2.5.

Exercise 5.2.8. Let Δ be a quadratic discriminant.

a) Suppose that

$$\varepsilon_\Delta = \frac{u_0 + v_0\sqrt{\Delta}}{2} \quad \text{and} \quad \varepsilon = \frac{u + v\sqrt{\Delta}}{2} \in \mathcal{O}_\Delta^\times\,, \quad \text{where } u,\, v \in \mathbb{N}.$$

Prove that $v_0 \,|\, v$.

b) Let p be a prime, and let $a,\, b,\, n \in \mathbb{Z}$ and $\sigma \in \{\pm 1\}$ such that $a^2 - 4\sigma = bp^2$ and $\Delta = p^2n^2 - 2an + b$. Prove that

$$\varepsilon = \frac{p^2n - a + p\sqrt{\Delta}}{2} \in \mathcal{O}_\Delta^\times\,, \quad \mathcal{N}(\varepsilon_\Delta) = \sigma\,,$$

and either $\varepsilon = \varepsilon_\Delta$ or $\Delta = d^2 \pm 4$ for some $d \in \mathbb{Z}$. Discuss some numerical examples. (Compare [**115**], [**116**] and [**80**].)

The following Theorem 5.2.9 is a powerful tool for recovering real quadratic orders with large class numbers. For historical details and applications we refer to [**74**, Ch. 3 and Ch. 5].

Theorem 5.2.9. *Let* $\Delta > 0$ *be a quadratic discriminant and* $\alpha \in \mathcal{O}_\Delta^\bullet$. *Then*

$$|\mathcal{N}(\alpha)| \ge \frac{u-e-1}{v^2}, \quad \textit{where} \quad \varepsilon_\Delta = \frac{u+v\sqrt{\Delta}}{2} \quad \textit{and} \quad \mathcal{N}(\varepsilon_\Delta) = e \in \{\pm 1\}\,.$$

Proof. The assertion is trivial for $\Delta = 5$. Hence we may assume that $\Delta > 5$ and thus $u \ge 2$. Suppose that

$$\alpha = \frac{x+y\sqrt{\Delta}}{2}, \quad \text{where } \ x,\, y \in \mathbb{N}_0\,,\ y \ \text{ is minimal, and } \ t = |\mathcal{N}(\alpha)|\,.$$

Then it follows that $x^2 - \Delta y^2 = 4\delta t$ for some $\delta \in \{\pm 1\}$,

$$\alpha_1 = e\varepsilon_\Delta^{-1}\alpha = \frac{x+y\sqrt{\Delta}}{2}\,\frac{u-v\sqrt{\Delta}}{2} = \frac{1}{2}\Bigl(\frac{xu-yv\Delta}{2} + \frac{yu-xv}{2}\sqrt{\Delta}\Bigr) \in \mathcal{O}_\Delta\,,$$

and since $\mathfrak{a} = \alpha_1\mathcal{O}_\Delta$, we obtain (by the minimal choice of y)

$$\Bigl|\frac{yu-xv}{2}\Bigr| \ge y\,, \quad \text{hence} \quad x \le \frac{y(u-2)}{v} \quad \text{or} \quad x \ge \frac{y(u+2)}{v}\,.$$

In the first case, it follows that

$$4\delta t = x^2 - \Delta y^2 \le \frac{y^2}{v^2}\,(u^2-4u+4) - \Delta y^2 = \frac{y^2}{v^2}\,(4e-4u+4)\,,$$

hence

$$\delta t \le \frac{y^2}{v^2}\,(e-u+1)\,, \quad \text{and therefore} \quad t \ge \frac{y^2}{v^2}\,(u-e-1) \ge \frac{u-e-1}{v^2}\,,$$

since $e-u+1 \le 0$. In the second case, we obtain

$$4\delta t = x^2 - \Delta y^2 \ge \frac{y^2}{v^2}\,(u^2+4u+4) - \Delta y^2 = \frac{y^2}{v^2}\,(4e+4u+4)\,,$$

hence

$$\delta t \ge \frac{y^2}{v^2}\,(e+u+1)\,, \quad \text{and therefore} \quad t \ge \frac{y^2}{v^2}\,(u+e+1) \ge \frac{u-e-1}{v^2}\,,$$

since $e+1 \ge -e-1$. □

With the aid of the unit group $\mathcal{O}_\Delta^\times$ we can now determine the algebraic structure of the stabilizer group of a quadratic irrational of discriminant Δ (as investigated in Theorem 1.2.2).

Theorem 5.2.10. *Let* ξ *be a quadratic irrational of type* (a,b,c) *and discriminant* Δ. *Then there is an isomorphism* $\Phi\colon \mathcal{O}_\Delta^\times \xrightarrow{\sim} \mathrm{Stab}(\xi)$, *given by*

$$\Phi\Bigl(\frac{x+y\sqrt{\Delta}}{2}\Bigr) = \begin{pmatrix} \frac{1}{2}(x+by) & -cy \\ ay & \frac{1}{2}(x-by) \end{pmatrix} \quad \textit{for all} \quad \varepsilon = \frac{x+y\sqrt{\Delta}}{2} \in \mathcal{O}_\Delta^\times\,,$$

and $\Phi(\mathcal{O}_\Delta^{\times +}) = \mathrm{Stab}^+(\xi)$.

Proof. By the Theorems 5.2.1 and 1.2.2, the map $\Phi\colon \mathcal{O}_\Delta^\times \to \mathrm{Stab}(\xi)$ is bijective and satisfies $\Phi(\mathcal{O}_\Delta^{\times+}) = \mathrm{Stab}^+(\xi)$. A simple (but lengthy) calculation shows that $\Phi(\varepsilon_1\varepsilon_2) = \Phi(\varepsilon_1)\Phi(\varepsilon_2)$ for all $\varepsilon_1,\, \varepsilon_2 \in \mathcal{O}_\Delta^\times$. Hence Φ is an isomorphism. □

5.3. Lattices and (invertible) fractional ideals in quadratic orders

We start this section with a parametrization of lattices and their rings of multipliers by means of quadratic irrationals (Theorem 5.3.1). This parametrization will be the main tool for the arithmetic investigations of ideals and ideal classes in the following sections. After that, we introduce (invertible) fractional ideals and derive their elementary algebraic properties. Although the notion of a (fractional) invertible ideal is a general concept in multiplicative ideal theory, we restrict here to the case of quadratic orders. For a more general approach we refer the reader to textbooks on ideal theory (e.g., [**65**]). Several results however, in particular the subsequent Theorem 5.3.5, are typical for quadratic orders and not valid in a more general context.

Theorem 5.3.1. *Let K be a quadratic number field.*

1. *If $\mathfrak{a}$ is a lattice in K, then $\mathfrak{a} \cap \mathbb{Q} = m\mathbb{Z}$, where $m = \min(\mathfrak{a} \cap \mathbb{Q}_{>0}) \in \mathbb{Q}_{>0}$, and there exists some quadratic irrational $\xi \in K \setminus \mathbb{Q}$ such that $\mathfrak{a} = m[1,\xi]$.*
2. *Let $\xi \in K$ be a quadratic irrational of type (a,b,c) and discriminant Δ and $m \in \mathbb{Q}^\times$. Then $\mathfrak{a} = m[1,\xi]$ is a lattice in K, $\mathfrak{a}\mathfrak{a}' = m^2a^{-1}\mathcal{O}_\Delta$ and $\mathcal{R}(\mathfrak{a}) = \mathcal{O}_\Delta$.*
3. *Let $\xi,\, \xi_1 \in K$ be quadratic irrationals and $m,\, m_1 \in \mathbb{Q}^\times$. Then we have $m[1,\xi] = m_1[1,\xi_1]$ if and only if $|m_1| = |m|$ and $\xi_1 = \delta\xi + \gamma$ for some $\delta \in \{\pm 1\}$ and $\gamma \in \mathbb{Z}$.*

Proof. 1. Let $\mathfrak{a}$ be a lattice in K and $\alpha \in \mathfrak{a}^\bullet$. Since $\mathcal{R}(\mathfrak{a})$ is a lattice, there exists some $q \in \mathbb{N}$ such that $q\alpha' \in \mathcal{R}(\mathfrak{a})$, and the $q\alpha'\alpha = q\mathcal{N}(\alpha) \in \mathfrak{a} \cap \mathbb{Q}^\times$. Hence $\mathfrak{a} \cap \mathbb{Q}$ is a non-zero finitely generated subgroup of $\mathbb{Q}$, and therefore $\mathfrak{a} \cap \mathbb{Q} = m\mathbb{Z}$, where $m = \min(\mathfrak{a} \cap \mathbb{Q}_{>0})$ (see Theorem A.4.2.2 and Corollary A.4.4).

Let (ω_1, ω_2) be a basis of $\mathfrak{a}$ and $c_1,\, c_2 \in \mathbb{Z}$ such that $m = c_1\omega_1 + c_2\omega_2$. We assert that $(d_1, d_2) = 1$. Indeed, if $d = (c_1, c_2)$, then $d^{-1}m = d^{-1}c_1\omega_1 + d^{-1}c_2\omega_2 \in \mathfrak{a} \cap \mathbb{Q}_{>0}$, and therefore $d = 1$. Let $u_1,\, u_2 \in \mathbb{Z}$ be such that $c_1u_1 - c_2u_2 = 1$. Then we obtain $\xi_1 = u_2\omega_1 + u_1\omega_2 \in \mathfrak{a}$,

$$\begin{pmatrix} m \\ \xi_1 \end{pmatrix} = \begin{pmatrix} c_1 & c_2 \\ u_2 & u_1 \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}, \quad \text{and since} \quad \det \begin{pmatrix} c_1 & c_2 \\ u_2 & u_1 \end{pmatrix} = 1\,,$$

it follows that $\mathfrak{a} = [m, \xi_1] = m[1, m^{-1}\xi_1]$.

2. By definition, $\mathfrak{a}$ is a lattice in K,

$$\mathcal{O}_\Delta\mathfrak{a} = m[1,\omega_\Delta]\,[1,\xi] = m[1,\omega_\Delta,\xi,\omega_\Delta\xi]\,, \quad \text{and} \quad \xi = \frac{b+\sqrt{\Delta}}{2a}\,.$$

Since

$$\omega_\Delta = \frac{\sigma_\Delta + \sqrt{\Delta}}{2} = \frac{\sigma_\Delta - b}{2} + \frac{b+\sqrt{\Delta}}{2} = \frac{\sigma_\Delta - b}{2} + a\xi \in [1,\xi]$$

and

$$\omega_\Delta\xi = \frac{(\sigma_\Delta + \sqrt{\Delta})(b+\sqrt{\Delta})}{4a} = -c + \frac{\sigma_\Delta + b}{2}\,\frac{b+\sqrt{\Delta}}{2a} = -c + \frac{\sigma_\Delta + b}{2}\,\xi \in [1,\xi]\,,$$

it follows that $\mathcal{O}_\Delta\mathfrak{a} \subset m[1,\xi] = \mathfrak{a}$, and therefore $\mathcal{O}_\Delta \subset \mathcal{R}(\mathfrak{a})$. Observing that $(a,b,c)=1$, we obtain

$$\begin{aligned} m^{-2}a\mathfrak{a}\mathfrak{a}' &= a[1,\xi]\,[1,\xi'] = [a, a\xi, a\xi', a\xi\xi'] = \Bigl[a, \frac{b+\sqrt{\Delta}}{2}, \frac{b-\sqrt{\Delta}}{2}, c\Bigr] \\ &= \Bigl[a, b, c, \frac{b+\sqrt{\Delta}}{2}\Bigr] = \Bigl[1, \frac{b+\sqrt{\Delta}}{2}\Bigr] = [1,\omega_\Delta] = \mathcal{O}_\Delta\,, \end{aligned}$$

hence $\mathcal{R}(\mathfrak{a}) = \mathcal{O}_\Delta\mathcal{R}(\mathfrak{a}) = m^{-2}a\mathfrak{a}\mathfrak{a}'\mathcal{R}(\mathfrak{a}) = m^{-2}a\mathfrak{a}\mathfrak{a}' = \mathcal{O}_\Delta$ and $\mathfrak{a}\mathfrak{a}' = m^2a^{-1}\mathcal{O}_\Delta$.

3. Suppose first that $\mathfrak{a} = m[1,\xi] = m_1[1,\xi_1]$. Then $\mathfrak{a}\cap\mathbb{Q} = m\mathbb{Z} = m_1\mathbb{Z}$, hence $|m| = |m_1|$ and $[1,\xi] = [1,\xi_1]$. In particular, this implies

$$\begin{pmatrix}1\\ \xi_1\end{pmatrix} = \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\begin{pmatrix}1\\ \xi\end{pmatrix} \quad \text{for some} \quad \begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in \mathsf{GL}_2(\mathbb{Z})\,.$$

By the linear independence of $(1,\xi)$ we obtain $\alpha = 1$ and $\beta = 0$, hence $\delta \in \{\pm 1\}$ and $\xi_1 = \delta\xi + \gamma$.

Conversely, if $|m| = |m_1|$ and $\xi_1 = \delta\xi+\gamma$ for some $\delta \in \{\pm1\}$ and $\gamma\in\mathbb{Z}$, then it follows immediately that $m[1,\xi] = |m|[1,\xi] = |m_1|[1,\xi_1] = m_1[1,\xi_1]$. □

Exercise 5.3.2. Let Δ be a quadratic discriminant, $d,\ e \in \mathbb{N}$ and $f = de$. Prove that $\mathfrak{a} = d\mathcal{O}_\Delta \cap \mathcal{O}_{\Delta f^2}$ is an ideal of $\mathcal{O}_{\Delta f^2}$, and $\mathcal{R}(\mathfrak{a}) = \mathcal{O}_{\Delta e^2}$.

Definition 5.3.3. Let Δ be a quadratic discriminant and $K = \mathbb{Q}(\sqrt{\Delta}\,)$.

- By a *fractional $\mathcal{O}_\Delta$-ideal* we mean a lattice $\mathfrak{a}$ of K such that $\mathcal{O}_\Delta\mathfrak{a} \subset \mathfrak{a}$ [equivalently, $\mathcal{O}_\Delta \subset \mathcal{R}(\mathfrak{a})$].
- A fractional $\mathcal{O}_\Delta$-ideal $\mathfrak{a}$ is called *$\mathcal{O}_\Delta$-invertible* if there exists a fractional $\mathcal{O}_\Delta$-ideal $\mathfrak{a}_1$ such that $\mathfrak{a}\mathfrak{a}_1 = \mathcal{O}_\Delta$.

If $\lambda \in K^\times$, then $\lambda\mathcal{O}_\Delta$ is an $\mathcal{O}_\Delta$-invertible fractional $\mathcal{O}_\Delta$-ideal [indeed, $(\lambda, \lambda\omega_\Delta)$ is a basis contained in $\lambda\mathcal{O}_K$, and $(\lambda\mathcal{O}_K)(\lambda^{-1}\mathcal{O}_K) = \mathcal{O}_K$]. We call $\lambda\mathcal{O}_K$ the *fractional principal ideal* generated by λ and $\mathcal{O}_K$ itself the *unit ideal.*

Before we proceed with the general theory, we gather the elementary properties of (invertible) fractional ideals.

Lemma 5.3.4. *Let Δ be a quadratic discriminant and $K = \mathbb{Q}(\sqrt{\Delta})$.*

1. *If $\mathfrak{a}$ and $\mathfrak{b}$ are fractional $\mathcal{O}_\Delta$-ideals and $\lambda \in K^\times$, then $\lambda\mathfrak{a}$, $\mathfrak{a}\cap\mathfrak{b}$, $\mathfrak{a}\mathfrak{b}$, $\mathfrak{a}+\mathfrak{b}$ and $(\mathfrak{a}:_K\mathfrak{b})$ are also fractional $\mathcal{O}_\Delta$-ideals, and $\mathfrak{a}$ is $\mathcal{O}_\Delta$-invertible if and only if $\lambda\mathfrak{a}$ is $\mathcal{O}_\Delta$-invertible.*
2. *For a subset $\mathfrak{a}$ of K, the following assertions are equivalent:*
   (a) *$\mathfrak{a}$ is a fractional $\mathcal{O}_\Delta$-ideal.*
   (b) *There is some $m \in \mathbb{N}$ such that $m\mathfrak{a}$ is a non-zero ideal of $\mathcal{O}_\Delta$.*
   (c) *There is some $\alpha \in \mathcal{O}_\Delta$ such that $\alpha\mathfrak{a}$ is a non-zero ideal of $\mathcal{O}_\Delta$.*

3. *If* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are fractional* $\mathcal{O}_\Delta$*-ideals such that* $\mathfrak{a}\mathfrak{b} = \mathcal{O}_\Delta$*, then* $\mathfrak{b} = (\mathcal{O}_\Delta :_K \mathfrak{a})$*. In particular,* $\mathfrak{a}$ *is* $\mathcal{O}_\Delta$*-invertible if and only if* $\mathfrak{a}(\mathcal{O}_\Delta :_K \mathfrak{a}) = \mathcal{O}_\Delta$*.*
4. *If* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are fractional* $\mathcal{O}_\Delta$*-ideals, then* $\mathfrak{a}\mathfrak{b}$ *is* $\mathcal{O}_\Delta$*-invertible if and only if both* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are* $\mathcal{O}_\Delta$*-invertible, and then* $(\mathcal{O}_\Delta :_K \mathfrak{a}\mathfrak{b}) = (\mathcal{O}_\Delta :_K \mathfrak{a})(\mathcal{O}_\Delta :_K \mathfrak{b})$*.*

PROOF. 1. Let $\mathfrak{a}$ and $\mathfrak{b}$ be fractional $\mathcal{O}_\Delta$-ideals and $\lambda \in K^\times$. Then $\lambda\mathfrak{a}$, $\mathfrak{a}\cap\mathfrak{b}$, $\mathfrak{a}\mathfrak{b}$, $\mathfrak{a}+\mathfrak{b}$ and $(\mathfrak{a} :_K \mathfrak{b})$ are lattices, $\mathcal{O}_\Delta(\lambda\mathfrak{a}) \subset \mathcal{O}_\Delta\mathfrak{a} \subset \mathfrak{a}$, $\mathcal{O}_\Delta(\mathfrak{a}\cap\mathfrak{b}) \subset \mathcal{O}_\Delta\mathfrak{a}\cap\mathcal{O}_\Delta\mathfrak{b} \subset \mathfrak{a}\cap\mathfrak{b}$, $\mathcal{O}_\Delta\mathfrak{a}\mathfrak{b} \subset \mathfrak{a}\mathfrak{b}$ and $\mathcal{O}_\Delta(\mathfrak{a}+\mathfrak{b}) \subset \mathcal{O}_\Delta\mathfrak{a}+\mathcal{O}_\Delta\mathfrak{b} \subset \mathfrak{a}+\mathfrak{b}$. Hence $\mathfrak{a}\cap\mathfrak{b}$, $\mathfrak{a}\mathfrak{b}$ and $\mathfrak{a}+\mathfrak{b}$ are fractional $\mathcal{O}_\Delta$-ideals.

If $\alpha \in \mathcal{O}_\Delta$ and $\beta \in (\mathfrak{a} :_K \mathfrak{b})$, then $\beta\mathfrak{b} \subset \mathfrak{a}$, hence $\alpha\beta\mathfrak{b} \subset \alpha\mathfrak{a} \subset \mathfrak{a}$, and thus $\alpha\beta \in (\mathfrak{a} :_K \mathfrak{b})$. This proves that $\mathcal{O}_\Delta(\mathfrak{a} :_K \mathfrak{b}) \subset (\mathfrak{a} :_K \mathfrak{b})$, and therefore $(\mathfrak{a} :_K \mathfrak{b})$ is a fractional $\mathcal{O}_\Delta$-ideal.

If $\mathfrak{a}$ is $\mathcal{O}_\Delta$-invertible and $\mathfrak{a}_1$ is a fractional $\mathcal{O}_\Delta$-ideal such that $\mathfrak{a}\mathfrak{a}_1 = \mathcal{O}_\Delta$, then $\lambda^{-1}\mathfrak{a}_1$ is also a fractional $\mathcal{O}_\Delta$-ideal and $(\lambda\mathfrak{a})(\lambda^{-1}\mathfrak{a}_1) = \mathcal{O}_\Delta$. Hence $\lambda\mathfrak{a}$ is also $\mathcal{O}_\Delta$-invertible. The converse follows since $\mathfrak{a} = \lambda^{-1}(\lambda\mathfrak{a})$.

2. (a) $\Rightarrow$ (b) Let $m \in \mathbb{N}$ be such that $m\mathfrak{a} \subset \mathcal{O}_\Delta$. Since $\mathcal{O}_\Delta \subset \mathcal{R}(\mathfrak{a}) = \mathcal{R}(m\mathfrak{a})$, it follows that $m\mathfrak{a}$ is an ideal of $\mathcal{O}_\Delta$.

(b) $\Rightarrow$ (c) $\Rightarrow$ (a) Obvious.

3. If $\mathfrak{a}\mathfrak{b} = \mathcal{O}_\Delta$, then $\mathfrak{b} \subset (\mathcal{O}_\Delta :_K \mathfrak{a}) = (\mathcal{O}_\Delta :_K \mathfrak{a})\mathfrak{a}\mathfrak{b} \subset \mathfrak{b}$, hence $(\mathcal{O}_\Delta :_K \mathfrak{a}) = \mathfrak{b}$.

4. Let $\mathfrak{a}$ and $\mathfrak{b}$ be fractional $\mathcal{O}_\Delta$-ideals. If both are $\mathcal{O}_\Delta$-invertible, then there exist fractional $\mathcal{O}_\Delta$-ideals $\mathfrak{a}_1$, $\mathfrak{b}_1$ such that $\mathfrak{a}\mathfrak{a}_1 = \mathfrak{b}\mathfrak{b}_1 = \mathcal{O}_\Delta$, and thus $\mathfrak{a}\mathfrak{b}\mathfrak{a}_1\mathfrak{b}_1 = \mathcal{O}_\Delta$. Hence $\mathfrak{a}\mathfrak{b}$ is $\mathcal{O}_\Delta$-invertible, and $(\mathcal{O}_\Delta :_K \mathfrak{a}\mathfrak{b}) = \mathfrak{a}_1\mathfrak{b}_1 = (\mathcal{O}_\Delta :_K \mathfrak{a})(\mathcal{O}_\Delta :_K \mathfrak{b})$ by 3.

Conversely, if $\mathfrak{a}\mathfrak{b}$ is $\mathcal{O}_\Delta$-invertible, then there exists a fractional $\mathcal{O}_\Delta$-ideal $\mathfrak{c}$ such that $\mathfrak{a}\mathfrak{b}\mathfrak{c} = \mathcal{O}_\Delta$, which implies that both $\mathfrak{a}$ and $\mathfrak{b}$ are $\mathcal{O}_\Delta$-invertible. ☐

Theorem 5.3.5. *Let* Δ *be a quadratic discriminant.*

1. *For a fractional* $\mathcal{O}_\Delta$*-ideal* $\mathfrak{a}$*, the following assertions are equivalent:*
   (a) $\mathfrak{a}$ *is* $\mathcal{O}_\Delta$*-invertible.*
   (b) *For every fractional* $\mathcal{O}_\Delta$*-ideal* $\mathfrak{b}$ *such that* $\mathfrak{b} \subset \mathfrak{a}$*, there exists a unique ideal* $\mathfrak{c}$ *of* $\mathcal{O}_\Delta$ *such that* $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$*.*
   (c) *For all fractional* $\mathcal{O}_\Delta$*-ideals* $\mathfrak{b}$ *and* $\mathfrak{c}$*,* $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ *implies* $\mathfrak{b} = \mathfrak{c}$*.*
   (d) $\mathcal{R}(\mathfrak{a}) = \mathcal{O}_\Delta$*.*
2. Δ *is a fundamental discriminant if and only if every fractional* $\mathcal{O}_\Delta$*-ideal is* $\mathcal{O}_\Delta$*-invertible.*

PROOF. 1. (a) $\Rightarrow$ (b) Let $\mathfrak{a}_1$ be a fractional $\mathcal{O}_\Delta$-ideal such that $\mathfrak{a}_1\mathfrak{a} = \mathcal{O}_\Delta$, and let $\mathfrak{b}$ be a fractional $\mathcal{O}_\Delta$-ideal such that $\mathfrak{b} \subset \mathfrak{a}$. Then $\mathfrak{c} = \mathfrak{a}_1\mathfrak{b} \subset \mathfrak{a}_1\mathfrak{a} = \mathcal{O}_\Delta$. Hence $\mathfrak{c}$ is an ideal of $\mathcal{O}_\Delta$, and $\mathfrak{a}\mathfrak{c} = \mathfrak{a}\mathfrak{a}_1\mathfrak{b} = \mathfrak{b}$. It remains to prove uniqueness. If $\mathfrak{c}_1$ is any ideal of $\mathcal{O}_\Delta$ such that $\mathfrak{b} = \mathfrak{a}\mathfrak{c}_1$, then $\mathfrak{c} = \mathfrak{a}_1\mathfrak{b} = \mathfrak{a}_1\mathfrak{a}\mathfrak{c}_1 = \mathfrak{c}_1$.

(b) $\Rightarrow$ (c) Obvious by the uniqueness in (b).

(c) $\Rightarrow$ (d) Since $\mathfrak{a} = \mathfrak{a}\mathcal{R}(\mathfrak{a}) = \mathfrak{a}\mathcal{O}_\Delta$, it follows that $\mathcal{R}(\mathfrak{a}) = \mathcal{O}_\Delta$.

(d) $\Rightarrow$ (a) By Theorem 5.3.1, there exist a quadratic irrational ξ of type (a,b,c) and discriminant Δ_1 and some $m \in \mathbb{Q}^\times$ such that $\mathfrak{a} = m[1,\xi]$, $\mathfrak{a}\mathfrak{a}' = m^2a^{-1}\mathcal{O}_{\Delta_1}$ and

$\mathcal{R}(\mathfrak{a}) = \mathcal{O}_{\Delta_1}$. By Theorem 5.1.7.2 we obtain $\Delta_1 = \Delta$, and since $\mathfrak{a}(m^{-2}a\mathfrak{a}') = \mathcal{O}_\Delta$, it follows that $\mathfrak{a}$ is $\mathcal{O}_\Delta$-invertible.

2. We consider the quadratic number field $K = \mathbb{Q}(\sqrt{\Delta}\,)$.

If Δ is a fundamental discriminant and $\mathfrak{a}$ is a fractional $\mathcal{O}_\Delta$-ideal, then $\Delta = \Delta_K$, and $\mathcal{O}_K = \mathcal{O}_\Delta \subset \mathcal{R}(\mathfrak{a})$ implies $\mathcal{R}(\mathfrak{a}) = \mathcal{O}_\Delta$. Hence $\mathfrak{a}$ is $\mathcal{O}_\Delta$-invertible.

Conversely, if Δ is not a fundamental discriminant, then $\mathcal{O}_\Delta \subsetneq \mathcal{O}_K$, and if $\mathfrak{a}$ is a fractional $\mathcal{O}_K$-ideal, then $\mathfrak{a}$ is also a fractional $\mathcal{O}_\Delta$-ideal, but since $\mathcal{R}(\mathfrak{a}) = \mathcal{O}_K$, it follows that $\mathfrak{a}$ is not $\mathcal{O}_\Delta$-invertible. □

We pause for an algebraic consideration of our results. Let Δ be a quadratic discriminant, $K = \mathbb{Q}(\sqrt{\Delta}\,)$ and $\mathcal{L}(K)$ the multiplicative semigroup of all lattices in K. Let $\mathcal{F}_\Delta$ be the set of all fractional $\mathcal{O}_\Delta$-ideals and $\mathcal{I}_\Delta$ the set of all non-zero ideals of $\mathcal{O}_\Delta$. Then $\mathcal{I}_\Delta \subset \mathcal{F}_\Delta \subset \mathcal{L}(K)$ are subsemigroups, and $\mathcal{I}_\Delta$ and $\mathcal{F}_\Delta$ are monoids with unit element $\mathcal{O}_\Delta$. A fractional $\mathcal{O}_\Delta$-ideal $\mathfrak{a}$ is $\mathcal{O}_\Delta$-invertible if and only if it is an invertible element of the monoid $\mathcal{F}_\Delta$, and then $(\mathcal{O}_\Delta :_K \mathfrak{a})$ is its inverse in $\mathcal{F}_\Delta$. In particular, the unit group $\mathcal{F}_\Delta^\times$ of $\mathcal{F}_\Delta$ is the group of $\mathcal{O}_\Delta$-invertible fractional $\mathcal{O}_\Delta$-ideals. A non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_\Delta$ is $\mathcal{O}_\Delta$-invertible if and only if there exists an ideal $\mathfrak{a}_1$ of $\mathcal{O}_\Delta$ such that $\mathfrak{a}\mathfrak{a}_1$ is a non-zero principal ideal. The map $\partial\colon K^\times \to \mathcal{F}_\Delta^\times$, defined by $\partial(\lambda) = \lambda\mathcal{O}_\Delta$, is a group homomorphism with kernel $\operatorname{Ker}(\partial) = \mathcal{O}_\Delta^\times$.

If Δ_1 is a quadratic discriminant such that $\mathcal{O}_{\Delta_1} \subset \mathcal{O}_\Delta$, then $\mathcal{F}_\Delta$ is a submonoid of $\mathcal{F}_{\Delta_1}$, and $\mathcal{F}_\Delta^\times = \{\mathfrak{a} \in \mathcal{F}_{\Delta_1} \mid \mathcal{R}(\mathfrak{a}) = \mathcal{O}_\Delta\,\}$.

Exercise 5.3.6. Let Δ be a quadratic discriminant and $\mathfrak{a}$ a fractional $\mathcal{O}_\Delta$-ideal. Prove the equivalence of the following conditions:

(a) $\mathfrak{a}$ is $\mathcal{O}_\Delta$-invertible.
(b) There exists some lattice $\mathfrak{c}$ in K such that $\mathfrak{a}\mathfrak{c} = \mathcal{O}_\Delta$.
(c) For every fractional $\mathcal{O}_\Delta$-ideal $\mathfrak{b}$, there exists a (unique) fractional $\mathcal{O}_\Delta$-ideal $\mathfrak{c}$ such that $\mathfrak{b} = \mathfrak{a}\mathfrak{c}$.
(d) For every fractional $\mathcal{O}_\Delta$-ideal $\mathfrak{b}$ we have $(\mathcal{O}_\Delta : \mathfrak{a})\mathfrak{b} = (\mathfrak{b} : \mathfrak{a})$.
(e) For all fractional $\mathcal{O}_\Delta$-ideals $\mathfrak{b}$ and $\mathfrak{c}$, if $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a}\mathfrak{c}$, then $\mathfrak{b} \subset \mathfrak{c}$.

5.4. Structure of ideals in quadratic orders

The main objective of this section is to introduce regular ideals of quadratic orders and to investigate their structure in connection with quadratic irrationals.

Definition 5.4.1. Let Δ be a quadratic discriminant.

1. An element $\alpha \in \mathcal{O}_\Delta$ is called *$\mathcal{O}_\Delta$-primitive* if $e^{-1}\alpha \notin \mathcal{O}_\Delta$ for all integers $e \geq 2$.
2. An ideal $\mathfrak{a}$ of $\mathcal{O}_\Delta$ is called
   - *$\mathcal{O}_\Delta$-primitive* if $e^{-1}\mathfrak{a} \not\subset \mathcal{O}_\Delta$ for all integers $e \geq 2$,
   - *$\mathcal{O}_\Delta$-regular* if it is $\mathcal{O}_\Delta$-primitive and $\mathcal{O}_\Delta$-invertible.
3. For a non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_\Delta$ we call
   - $\mathfrak{N}_\Delta(\mathfrak{a}) = (\mathcal{O}_\Delta : \mathfrak{a})$ the *absolute norm* of $\mathfrak{a}$.

Note that $\mathfrak{N}_\Delta(\mathfrak{a}) < \infty$ (see Theorem A.4.2.4). If $\alpha \in \mathcal{O}_\Delta^\bullet$, then Theorem 5.1.3 (applied with $\mathfrak{c} = \mathfrak{a} = \mathcal{O}_\Delta$) shows that

$$\mathfrak{N}_\Delta(\alpha\mathcal{O}_\Delta) = |\mathcal{N}(\alpha)|\,,$$

which justifies the terminology.

If $\alpha \in \mathcal{O}_\Delta$, then the principal ideal $\alpha\mathcal{O}_\Delta$ is $\mathcal{O}_\Delta$-regular if and only if it is $\mathcal{O}_\Delta$-primitive. If $e \in \mathbb{N}$, then $e^{-1}\alpha\mathcal{O}_\Delta \subset \mathcal{O}_\Delta$ if and only if $e^{-1}\alpha \in \mathcal{O}_\Delta$. Hence $\alpha\mathcal{O}_\Delta$ is $\mathcal{O}_\Delta$-primitive if and only if α is $\mathcal{O}_\Delta$-primitive. If $a,\ b \in \mathbb{Z}$ and $\alpha = a + b\omega_\Delta$, then α is $\mathcal{O}_\Delta$-primitive if and only if $(a,b) = 1$.

Theorem 5.4.2 (Structure theorem for ideals in quadratic orders)**.** *Let Δ be a quadratic discriminant and $K = \mathbb{Q}(\sqrt{\Delta})$.*

1. *Let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_\Delta$. Then there exist integers $a,\ e \in \mathbb{N}$ and $b,\ c \in \mathbb{Z}$ such that*

   $$\mathfrak{a} = e\Big[a, \frac{b+\sqrt{\Delta}}{2}\Big] \quad \textit{and} \quad \Delta = b^2 - 4ac\,.$$

   Let $a,\ e,\ b,\ c$ be as above, $g = (a,b,c)$ and $\Delta_1 = g^{-2}\Delta$. Then the following assertions hold:

   - *$ae = \min(\mathfrak{a} \cap \mathbb{N})$, $\mathfrak{a} \cap \mathbb{Z} = ae\mathbb{Z}$, $ae^2 = \mathfrak{N}_\Delta(\mathfrak{a}) \in \mathfrak{a}$ and $g \,|\, \mathfrak{N}_\Delta(\mathfrak{a})$;*
   - *$e^{-1}\mathfrak{a}$ is $\mathcal{O}_\Delta$-primitive, and if $\theta\colon K \to \mathbb{Q}$ is defined by $\theta(x+y\sqrt{\Delta}) = 2y$ for all $x,\ y \in \mathbb{Q}$, then $\theta(\mathfrak{a}) = e\mathbb{Z}$;*
   - *Δ_1 is a quadratic discriminant, $\mathfrak{a}\mathfrak{a}' = g\mathfrak{N}_\Delta(\mathfrak{a})\mathcal{O}_{\Delta_1}$, $\mathcal{R}(\mathfrak{a}) = \mathcal{O}_{\Delta_1}$, and $(\mathcal{R}(\mathfrak{a}){:}\mathcal{O}_\Delta) = g$;*
   - *$\mathfrak{a}$ is $\mathcal{O}_\Delta$-primitive if and only if $e = 1$, $\mathfrak{a}$ is $\mathcal{O}_\Delta$-invertible if and only if $g = 1$, and $\mathfrak{a}$ is $\mathcal{O}_\Delta$-regular if and only if $e = g = 1$.*

2. *Let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_\Delta$. If $a,\ a_1,\ e,\ e_1 \in \mathbb{N}$ and $b,\ b_1 \in \mathbb{Z}$ are integers, then*

   $$\mathfrak{a} = e\Big[a, \frac{b+\sqrt{\Delta}}{2}\Big] = e_1\Big[a_1, \frac{b_1+\sqrt{\Delta}}{2}\Big]$$

   holds if and only if $a = a_1$, $e = e_1$ and $b \equiv b_1 \bmod 2a$.

3. *Let $a,\ b,\ e$ be integers such that $ae \ne 0$, and*

   $$\mathfrak{a} = \Big[a, \frac{b+e\sqrt{\Delta}}{2}\Big]\,.$$

   Then $\mathfrak{a}$ is an ideal of $\mathcal{O}_\Delta$ if and only if

   $$e \,|\, a\,, \quad 2e \,|\, e\Delta - b \quad \textit{and} \quad 4ae \,|\, b^2 - \Delta e^2\,.$$

   Moreover, if this is the case, then $\mathfrak{a}$ is $\mathcal{O}_\Delta$-primitive if and only if $|e| = 1$, and $\mathfrak{a}$ is $\mathcal{O}_\Delta$-regular if and only if

   $$|e| = 1 \quad \textit{and} \quad \Big(a, b, \frac{b^2-\Delta}{4a}\Big) = 1\,.$$

Proof. 1. By Theorem 5.3.1, there exists some $\xi \in K\setminus\mathbb{Q}$ such that $\mathfrak{a} = m[1,\xi]$, where $m = \min(\mathfrak{a}\cap\mathbb{Q}_{>0})$. Since $\mathfrak{a}\cap\mathbb{Q} \subset \mathcal{O}_\Delta\cap\mathbb{Q} = \mathbb{Z}$, it follows that $m \in \mathbb{N}$. Suppose that ξ is of type (a_0,b_0,c_0) and discriminant $\Delta_0 = b_0^2 - 4a_0c_0$. Then we obtain $\mathcal{R}(\mathfrak{a}) = \mathcal{O}_{\Delta_0} \supset \mathcal{O}_\Delta$, and if $g = (\mathcal{R}(\mathfrak{a}) : \mathcal{O}_\Delta)$, then $\Delta = \Delta_0 g^2$ by Theorem 5.1.7.2. Now we set $a = a_0g$, $b = b_0g$ and $c = c_0g$. Then $(a,b,c) = g$, $\Delta = b^2-4ac$, and

$$\xi = \frac{b_0+\sqrt{\Delta_0}}{2a_0} = \frac{b+\sqrt{\Delta}}{2a}\,.$$

Since $m\xi \in \mathfrak{a} \subset \mathcal{O}_\Delta$, it follows that $a\,|\,m$, say $m = ae$, where $e \in \mathbb{N}$, and then

$$\mathfrak{a} = m[1,\xi] = ae\Big[1, \frac{b+\sqrt{\Delta}}{2a}\Big] = e\Big[a, \frac{b+\sqrt{\Delta}}{2}\Big], \quad \text{as asserted.}$$

Assume now that a, $e \in \mathbb{N}$ and b, $c \in \mathbb{Z}$ are any integers such that

$$\mathfrak{a} = e\Big[a, \frac{b+\sqrt{\Delta}}{2}\Big], \quad g = (a,b,c)\,, \quad \Delta = b^2-4ac \ \text{ and } \ \Delta_1 = g^{-2}\Delta\,.$$

Then $(ae, e(b+\sqrt{\Delta})/2)$ is a basis of $\mathfrak{a}$. Hence $\mathfrak{a}\cap\mathbb{Z} = ae\mathbb{Z}$, $ae = \min(\mathfrak{a}\cap\mathbb{N})$, and

$$\begin{pmatrix} ae \\ e\dfrac{b+\sqrt{\Delta}}{2}\end{pmatrix} = \begin{pmatrix} ae & 0 \\ e\dfrac{b-\sigma_\Delta}{2} & e\end{pmatrix}\begin{pmatrix}1\\ \omega_\Delta\end{pmatrix}.$$

Now it follows that

$$\mathfrak{N}_\Delta(\mathfrak{a}) = (\mathcal{O}_\Delta : \mathfrak{a}) = \Big([1,\omega_\Delta] : \Big[ae,\, e\frac{b+\sqrt{\Delta}}{2}\Big]\Big) = \det\begin{pmatrix} ae & 0 \\ e\dfrac{b-\sigma_\Delta}{2} & e\end{pmatrix} = ae^2 \in \mathfrak{a}$$

(by Theorem A.4.2.4), and $g\,|\,a\,|\,\mathfrak{N}_\Delta(\mathfrak{a})$. By definition,

$$\mathfrak{a} = \Big\{aeu + \frac{b+\sqrt{\Delta}}{2}ev \,\Big|\, u,\, v \in \mathbb{Z}\Big\}, \quad \theta\Big(aeu + \frac{b+\sqrt{\Delta}}{2}ev\Big) = ev \ \text{ for all } u,\, v \in \mathbb{Z}\,,$$

and therefore $\theta(\mathfrak{a}) = e\mathbb{Z}$. If $e_1 \in \mathbb{N}$, then

$$e_1^{-1}(e^{-1}\mathfrak{a}) = \Big[\frac{a}{e_1}, \frac{b+\sqrt{\Delta}}{2e_1}\Big]$$

and $e_1^{-1}(e^{-1}\mathfrak{a}) \subset \mathcal{O}_\Delta$ implies $e_1 = 1$. Hence $e^{-1}\mathfrak{a}$ is $\mathcal{O}_\Delta$-primitive.

If $a = ga_1$, $b = gb_1$ and $c = gc_1$, where a_1, b_1, $c_1 \in \mathbb{Z}$, then $(a_1,b_1,c_1) = 1$, and $\Delta_1 = g^{-2}\Delta = b_1^2 - 4a_1c_1$ is a quadratic discriminant. Hence $(\mathcal{O}_{\Delta_1} : \mathcal{O}_\Delta) = g$, and

$$\xi = \frac{b_1+\sqrt{\Delta_1}}{2a_1} = \frac{b+\sqrt{\Delta}}{2a} \ \text{ is of type } \ (a_1,b_1,c_1) \ \text{ and discriminant } \ \Delta_1\,.$$

Since $\mathfrak{a} = ae[1,\xi]$, Theorem 5.3.1.2 implies that $\mathcal{R}(\mathfrak{a}) = \mathcal{O}_{\Delta_1}$ and

$$\mathfrak{a}\mathfrak{a}' = (ae)^2a_1^{-1}\mathcal{O}_{\Delta_1} = gae^2\mathcal{O}_{\Delta_1} = g\mathfrak{N}_\Delta(\mathfrak{a})\mathcal{O}_{\Delta_1}\,.$$

By Theorem 5.3.5, $\mathfrak{a}$ is $\mathcal{O}_\Delta$-invertible if and only if $\mathcal{O}_\Delta = \mathcal{O}_{\Delta_1}$, that is, if and only if $g = 1$. Since the ideal $\mathfrak{a}$ is $\mathcal{O}_\Delta$-primitive if and only if $e = 1$, it is $\mathcal{O}_\Delta$-regular if and only if $e = g = 1$.

2. Assume first that a, a_1, e, $e_1 \in \mathbb{N}$ and b, $b_1 \in \mathbb{Z}$ are such that

$$\mathfrak{a} = e\Big[\,a,\,\frac{b+\sqrt{\Delta}}{2}\,\Big] = e_1\Big[\,a_1,\,\frac{b_1+\sqrt{\Delta}}{2}\,\Big]\,.$$

Then it follows that $ae = \min(\mathfrak{a}\cap\mathbb{N}) = a_1e_1$ and $\theta(\mathfrak{a}) = e\mathbb{Z} = e_1\mathbb{Z}$. Hence we obtain $a = a_1$, $e = e_1$, and

$$\Big[a,\,\frac{b+\sqrt{\Delta}}{2}\Big] = \Big[a,\,\frac{b_1+\sqrt{\Delta}}{2}\Big] \quad \text{implies} \quad \frac{b+\sqrt{\Delta}}{2} = au + \frac{b_1+\sqrt{\Delta}}{2}v$$

for some u, $v \in \mathbb{Z}$, and therefore $b = 2au + b_1 \equiv b_1 \bmod 2a$.

Conversely, assume that $a = a_1$, $e = e_1$ and $b \equiv b_1 \bmod 2a$, say $b = b_1 + 2au$ for some $u \in \mathbb{Z}$. Then

$$\frac{b+\sqrt{\Delta}}{2} = au + \frac{b_1+\sqrt{\Delta}}{2} \in \Big[a,\,\frac{b_1+\sqrt{\Delta}}{2}\Big], \quad \text{hence} \quad \Big[a,\,\frac{b+\sqrt{\Delta}}{2}\Big] \subset \Big[a,\,\frac{b_1+\sqrt{\Delta}}{2}\Big],$$

and thus equality holds by symmetry.

3. Assume first that $e \mid a$, $2e \mid e\Delta - b$ and $4ae \mid b^2 - \Delta e^2$. Then $e \mid b$, and since $e\Delta \equiv b \bmod 2$, it follows that $\mathfrak{a} \subset \mathcal{O}_\Delta$. Let a_0, b_0, $c_0 \in \mathbb{Z}$ be such that $a = ea_0$, $b = eb_0$, $b^2 - \Delta e^2 = 4aec_0$, and set $g = (a_0, b_0, c_0)$. Then $a_0 = ga_1$, $b_0 = gb_1$ and $c_0 = gc_1$, where a_1, b_1, $c_1 \in \mathbb{Z}$ and $(a_1, b_1, c_1) = 1$. If $\Delta_1 = b_1^2 - 4a_1c_1$, then $\Delta = g^2\Delta_1$,

$$\xi = \frac{b_1 + \sqrt{\Delta_1}}{2a_1} = \frac{b + e\sqrt{\Delta}}{2a}$$

is a quadratic irrational of type (a_1, b_1, c_1) and discriminant Δ_1, and $\mathfrak{a} = a[1, \xi]$. Hence $\mathfrak{a}$ is a lattice in K, Theorem 5.3.1.2 implies $\mathcal{R}(\mathfrak{a}) = \mathcal{O}_{\Delta_1} \supset \mathcal{O}_\Delta$, and therefore $\mathfrak{a}$ is an ideal of $\mathcal{O}_\Delta$.

Let now $\mathfrak{a}$ be an ideal of $\mathcal{O}_\Delta$. Since

$$\Big[\,a,\,\frac{b+e\sqrt{\Delta}}{2}\,\Big] = \Big[\,|a|,\,\frac{b+e\sqrt{\Delta}}{2}\,\Big],$$

we may assume that $a > 0$. By 1., there exist a_1, $e_1 \in \mathbb{N}$ and b_1, $c_1 \in \mathbb{Z}$ such that $\Delta = b_1^2 - 4a_1c_1$ and

$$\mathfrak{a} = e_1\Big[a_1,\,\frac{b_1+\sqrt{\Delta}}{2}\Big], \quad \text{whence} \quad a_1e_1\Big[1,\,\frac{b_1+\sqrt{\Delta}}{2a_1}\Big] = a\Big[1,\,\frac{b+e\sqrt{\Delta}}{2a}\Big].$$

By Theorem 5.3.1.3 we obtain

$$a = a_1e_1\,, \quad \text{and} \quad \frac{b+e\sqrt{\Delta}}{2a} = \delta\,\frac{b_1+\sqrt{\Delta}}{2a_1} + \gamma \quad \text{for some } \delta \in \{\pm 1\} \text{ and } \gamma \in \mathbb{Z},$$

hence $e = \delta e_1$ and $b = \delta e_1 b_1 + 2a_1e_1\gamma = b_1e + 2a\gamma$. In particular, it follows that $a = a_1\delta e$ and consequently $e \mid a$. Now we calculate

$$e\Delta - b = e(b_1^2 - 4a_1c_1 - b_1 - 2\gamma\delta a_1)\,,$$

hence $2e \mid e\Delta - b$, and $b^2 - \Delta e^2 = 4ae(a_1\delta\gamma^2 + b_1\gamma + c_1)$, which implies $4ae \mid b^2 - \Delta e^2$.

By 1., $\mathfrak{a}$ is $\mathcal{O}_\Delta$-primitive if and only if $e_1 = |e| = 1$. In this case

$$g = \Big(a, b, \frac{b^2-\Delta}{4a}\Big) = (a_1\delta e,\ b_1e + 2a_1e_1\gamma,\ a_1\delta\gamma^2 + b_1\gamma + c_1) = (a_1, b_1, c_1)\,,$$

and, again by 1., $\mathfrak{a}$ is $\mathcal{O}_\Delta$-regular if and only if $g = 1$. □

Corollary 5.4.3. *Let* Δ *be a quadratic discriminant,* f_Δ *its conductor and* $\mathfrak{a}$ *a non-zero ideal of* $\mathcal{O}_\Delta$*.*

1. $\mathfrak{a}$ *is* $\mathcal{O}_\Delta$*-invertible if and only if* $\mathfrak{a}\mathfrak{a}' = \mathfrak{N}_\Delta(\mathfrak{a})\mathcal{O}_\Delta$*.*
2. *If* $(\mathfrak{N}_\Delta(\mathfrak{a}), f_\Delta) = 1$*, then* $\mathfrak{a}$ *is* $\mathcal{O}_\Delta$*-invertible.*

Proof. 1. By Theorem 5.4.2.1, $\mathfrak{a}\mathfrak{a}' = (\mathcal{R}(\mathfrak{a}){:}\mathcal{O}_\Delta)\mathfrak{N}_\Delta(\mathfrak{a})\mathcal{R}(\mathfrak{a}) \supset \mathfrak{N}_\Delta(\mathfrak{a})\mathcal{O}_\Delta$, and equality holds if and only if $\mathcal{R}(\mathfrak{a}) = \mathcal{O}_\Delta$. Hence the assertion follows by Theorem 5.3.5.

2. If $g = (\mathcal{R}(\mathfrak{a}) : \mathcal{O}_\Delta)$, then $g \,|\, (\mathcal{O}_K : \mathcal{O}_\Delta) = f_\Delta$, and, by Theorem 5.4.2.2, g divides $\mathfrak{N}_\Delta(\mathfrak{a})$. Consequently, if $(\mathfrak{N}_\Delta(\mathfrak{a}), f_\Delta) = 1$, then $g = 1$, hence $\mathcal{O}_\Delta = \mathcal{R}(\mathfrak{a})$, and thus $\mathfrak{a}$ is $\mathcal{O}_\Delta$-invertible. $\square$

Exercise 5.4.4. Let $\Delta = 4D + \sigma$ be a quadratic discriminant, where $D \in \mathbb{Z}$ and $\sigma \in \{0,1\}$. Let $\alpha \in \mathcal{O}_\Delta$ be primitive, and

$$\alpha = \frac{u + v\sqrt{\Delta}}{2}, \quad \text{where} \quad u,\, v \in \mathbb{Z} \ \text{ and } \ u \equiv v\sigma \bmod 2\,.$$

Prove that there exist $w,\, z \in \mathbb{Z}$ such that

$$vw + \frac{u + \sigma v}{2} z = 1\,,$$

and then

$$\alpha\mathcal{O}_\Delta = \Big[\frac{|u^2 - v^2\Delta|}{4}, \frac{b + \sqrt{\Delta}}{2}\Big], \quad \text{where } b = uw + \frac{u\sigma + v\Delta}{2} z \in \mathbb{Z}\,.$$

Theorem and Definition 5.4.5. *Let* Δ *be a quadratic discriminant.*

1. *Let* ξ *be a quadratic irrational of type* (a,b,c) *and discriminant* Δ*. Then the lattice*
$$I(\xi) = a[1,\xi] = \Big[|a|, \frac{b + \sqrt{\Delta}}{2}\Big]$$
is an $\mathcal{O}_\Delta$*-regular ideal,* $\mathfrak{N}_\Delta(I(\xi)) = |a|$*,* $I(-\xi) = I(\xi)$ *and* $I(\xi') = I(\xi)'$*.*
The ideal $I(\xi)$ is called the *ideal associated with* ξ.
2. *For every* $\mathcal{O}_\Delta$*-regular ideal* $\mathfrak{a}$ *there exists a quadratic irrational* ξ *of type* (a,b,c) *with* $a = \mathfrak{N}_\Delta(\mathfrak{a})$ *and discriminant* Δ *such that* $\mathfrak{a} = I(\xi)$*.*
3. *If* ξ *and* ξ_1 *are quadratic irrationals of discriminant* Δ*, then* $I(\xi) = I(\xi_1)$ *if and only if* $\xi_1 = \varepsilon\xi + n$ *for some* $\varepsilon \in \{\pm 1\}$ *and* $n \in \mathbb{Z}$*.*

Proof. 1. Since $\Delta = b^2 - 4ac$ and $(a,b,c) = 1$, Theorem 5.4.2.1 implies that

$$I(\xi) = a[1,\xi] = \Big[|a|, \frac{b + \sqrt{\Delta}}{2}\Big]$$

is an $\mathcal{O}_\Delta$-regular ideal, and $\mathfrak{N}_\Delta(I(\xi)) = |a|$. Since ξ' is of type $(-a,-b,-c)$ and $-\xi$ is of type $(-a,b,-c)$, it follows that

$$I(-\xi) = (-a)[1,-\xi] = a[1,\xi] = I(\xi) \quad \text{and} \quad I(\xi') = (-a)[1,\xi'] = a[1,\xi]' = I(\xi)'\,.$$

2. Let $\mathfrak{a}$ be an $\mathcal{O}_\Delta$-regular ideal and $a = \mathfrak{N}_\Delta(\mathfrak{a})$. By Theorem 5.4.2.1 there exist $b,\ c \in \mathbb{Z}$ such that $\Delta = b^2 - 4ac,\ \ (a,b,c) = 1$ and

$$\mathfrak{a} = \Big[a, \frac{b+\sqrt{\Delta}}{2}\Big] = I(\xi), \quad \text{where} \quad \xi = \frac{b+\sqrt{\Delta}}{2a}\,.$$

Clearly, ξ is of type (a,b,c) and discriminant Δ.

3. Let ξ and ξ_1 be quadratic irrationals of discriminant Δ, let ξ be of type (a,b,c) and ξ_1 of type (a_1,b_1,c_1). By Theorem 5.4.2.2 we obtain $I(\xi) = I(\xi_1)$ if and only if $|a| = |a_1|$ and $b_1 \equiv b \mod 2|a|$. However, this holds if and only if there exist some $n \in \mathbb{Z}$ and $\varepsilon \in \{\pm 1\}$ such that $a_1 = \varepsilon a$ and $b_1 = b + 2\varepsilon a n$, which is equivalent to $\xi_1 = \varepsilon\xi + n$. $\square$

We close this section with a general (and thus rather complicated) formula for the product of two $\mathcal{O}_\Delta$-ideals.

Theorem 5.4.6. *Let Δ be a quadratic discriminant and $K = \mathbb{Q}(\sqrt{\Delta})$. For $i \in \{1,2\}$, let $\mathfrak{a}_i$ be a non-zero ideal of $\mathcal{O}_\Delta$, say*

$$\mathfrak{a}_i = e_i\Big[a_i, \frac{b_i+\sqrt{\Delta}}{2}\Big], \quad \textit{where} \ \ a_i,\, e_i \in \mathbb{N}\,, \quad b_i,\, c_i \in \mathbb{Z} \ \ \textit{and} \ \ \Delta = b_i^2 - 4a_ic_i\,.$$

We set

$$s = \frac{b_1+b_2}{2}\,, \quad n = \frac{b_1-b_2}{2}\,, \quad e = (a_1,a_2,s)\,, \quad d = (e,c_1,c_2,n)\,, \quad a = \frac{da_1a_2}{e^2}\,,$$

and we choose $u,\ v,\ w \in \mathbb{Z}$ be such that $e = a_1u + a_2v + sw$. Then we have

$$\mathfrak{a}_1\mathfrak{a}_2 = ee_1e_2\Big[a, \frac{b+\sqrt{\Delta}}{2}\Big]\,, \quad \textit{where} \quad b = b_2 + \frac{2a_2}{d}\,[v(s-b_2) - wc_2]\,,$$

and $\mathfrak{N}_\Delta(\mathfrak{a}_1\mathfrak{a}_2) = d\,\mathfrak{N}_\Delta(\mathfrak{a}_1)\mathfrak{N}_\Delta(\mathfrak{a}_2)$.

If $(a_1,\, b_1,\, c_1,\, a_2,\, b_2,\, c_2) = 1$, then $\mathfrak{N}_\Delta(\mathfrak{a}_1\mathfrak{a}_2) = \mathfrak{N}_\Delta(\mathfrak{a}_1)\mathfrak{N}_\Delta(\mathfrak{a}_2)$. In particular, this holds if at least one of the ideals $\mathfrak{a}_1,\ \mathfrak{a}_2$ is $\mathcal{O}_\Delta$-invertible.

$\mathfrak{a}_1\mathfrak{a}_2$ is $\mathcal{O}_\Delta$-primitive if and only both $\mathfrak{a}_1$ and $\mathfrak{a}_2$ are $\mathcal{O}_\Delta$-primitive, and $e = 1$.

PROOF. We may assume that $e_1 = e_2 = 1$. Let $\theta\colon K \to \mathbb{Q}$ be defined by $\theta(x + y\sqrt{\Delta}) = 2y$ for all $x,\ y \in \mathbb{Q}$. Then Theorem 5.4.2 implies

$$\mathfrak{a}_1\mathfrak{a}_2 = C\Big[A, \frac{B+\sqrt{\Delta}}{2}\Big]\,,$$

where $A,\ C \in \mathbb{N}$ are such that $AC\mathbb{Z} = \mathfrak{a}_1\mathfrak{a}_2 \cap \mathbb{Z}$, $C\mathbb{Z} = \theta(\mathfrak{a}_1\mathfrak{a}_2)$, and $B \in \mathbb{Z}$ is any integer such that

$$\frac{B+\sqrt{\Delta}}{2} \in C^{-1}\mathfrak{a}_1\mathfrak{a}_2\,.$$

By definition, $\mathfrak{a}_1\mathfrak{a}_2 = [a_1a_2,\ \beta_2, \beta_3, \beta_4]$, where

$$\beta_2 = \frac{a_1b_2 + a_1\sqrt{\Delta}}{2}\,, \quad \beta_3 = \frac{a_2b_1 + a_2\sqrt{\Delta}}{2}$$

and

$$\beta_4 = \frac{(b_1+\sqrt{\Delta})(b_2+\sqrt{\Delta})}{4} = \frac{\frac{b_1b_2+\Delta}{2} + s\sqrt{\Delta}}{2} = \frac{b_2s - 2a_2c_2 + s\sqrt{\Delta}}{2}\,.$$

Hence $\theta(\mathfrak{a}_1\mathfrak{a}_2) = a_1\mathbb{Z} + a_2\mathbb{Z} + s\mathbb{Z} \subset \mathbb{Z}$, and therefore $C = (a_1,a_2,s) = e$.

$\mathfrak{a}_1\mathfrak{a}_2 \cap \mathbb{Z}$ consists of all numbers of the form $a_1a_2u_1 + \beta_2u_2 + \beta_3u_3 + \beta_4u_4$, where $(u_1, u_2, u_3, u_4) \in \mathbb{Z}^4$ satisfies the Diophantine equation $a_1u_2 + a_2u_3 + su_4 = 0$. By Theorem A.3.7, a triple $(u_2, u_3, u_4) \in \mathbb{Z}^3$ satisfies this Diophantine equation if and only if there is some $(U, V, W) \in \mathbb{Z}^3$ such that

$$u_2 = \frac{a_2}{(a_1,a_2)}\,V - \frac{s}{(a_1,s)}\,W\,, \quad u_3 = \frac{s}{(a_2,s)}\,U - \frac{a_1}{(a_1,a_2)}\,V$$

and

$$u_4 = \frac{a_1}{(a_1,s)}\,W - \frac{a_2}{(a_2,s)}\,U\,.$$

Hence $\mathfrak{a}_1\mathfrak{a}_2 \cap \mathbb{Z}$ consists of all numbers of the form

$$\begin{aligned} a_1a_2u_1 + \frac{a_2b_1 - a_2\frac{b_1b_2+\Delta}{2}}{2(a_2,s)}\,U + \frac{a_1a_2b_2 - a_1a_2b_1}{2(a_1,a_2)}\,V + \frac{a_1(b_2s - 2a_2c_2) - a_1b_2s}{2(a_1,s)}\,W \\ = a_1a_2u_1 + \frac{a_1a_2c_1}{(a_2,s)}\,U + \frac{a_1a_2n}{(a_1,a_2)}\,V - \frac{a_1a_2c_2}{(a_1,s)}\,W \end{aligned}$$

for some $(u_1, U, V, W) \in \mathbb{Z}^4$, and consequently

$$AC = \Big(a_1a_2,\, \frac{a_1a_2c_1}{(a_2,s)},\, \frac{a_1a_2c_2}{(a_1,s)},\, \frac{a_1a_2n}{(a_1,a_2)}\Big)\,.$$

Now we observe that

$$a_1c_1 - a_2c_2 = \frac{b_1^2 - \Delta}{4} - \frac{b_2^2 - \Delta}{4} = sn$$

and obtain

$$\begin{aligned} \frac{ec_1}{(a_2,s)} &= \frac{(a_2c_2 + sn)u + a_2c_1v + c_1sw}{(a_2,s)} \\ &= \frac{a_2}{(a_2,s)}\,c_2u + \frac{s}{(a_2,s)}\,nu + \frac{a_2}{(a_2,s)}\,c_1v + \frac{s}{(a_2,s)}\,c_1w\,, \\ \frac{ec_2}{(a_1,s)} &= \frac{a_1c_2u + (a_1c_1 - sn)v + c_2sw}{(a_1,s)} \\ &= \frac{a_1}{(a_1,s)}\,c_2u + \frac{a_1}{(a_1,s)}\,c_1v - \frac{s}{(a_1,s)}\,nv + \frac{s}{(a_1,s)}\,c_2w \qquad \text{and} \\ \frac{en}{(a_1,a_2)} &= \frac{a_1nu + a_2nv + (a_1c_1 - a_2c_2)w}{(a_1,a_2)} \\ &= \frac{a_1}{(a_1,a_2)}\,nu + \frac{a_2}{(a_1,a_2)}\,nv + \frac{a_1}{(a_1,a_2)}\,c_1w - \frac{a_2}{(a_1,a_2)}\,c_2w\,. \end{aligned}$$

These identities show that

$$\frac{ec_1}{(a_2,s)}\,,\ \frac{ec_2}{(a_1,s)}\,,\ \frac{en}{(a_1,a_2)} \in \mathbb{Z}$$

and

$$(c_1,c_2,n) \;\Big|\; \frac{ec_1}{(a_2,s)} \;\Big|\; c_1\,, \quad (c_1,c_2,n) \;\Big|\; \frac{ec_2}{(a_1,s)} \;\Big|\; c_2\,, \quad (c_1,c_2,n) \;\Big|\; \frac{en}{(a_1,a_2)} \;\Big|\; n\,.$$

Therefore it follows that

$$AC = \frac{a_1a_2}{e}\Bigl(e, \frac{ec_1}{(a_2,s)}, \frac{ec_2}{(a_1,s)}, \frac{en}{(a_1,a_2)}\Bigr) = \frac{a_1a_2}{e}(e,c_1,c_2,n) = \frac{a_1a_2d}{e},$$

$$A = \frac{AC}{C} = \frac{a_1a_2d}{e^2} = a \quad\text{and}\quad \mathfrak{N}_\Delta(\mathfrak{a}_1\mathfrak{a}_2) = ae^2 = da_1a_2 = d\mathfrak{N}_\Delta(\mathfrak{a}_1)\mathfrak{N}_\Delta(\mathfrak{a}_2).$$

To determine a possible value for b, we observe that

$$C^{-1}\mathfrak{a}_1\mathfrak{a}_2 = \mathbb{Z}\,\frac{a_1a_2d}{e^2} + \mathbb{Z}\,\frac{\beta_2}{e} + \mathbb{Z}\,\frac{\beta_3}{e} + \mathbb{Z}\,\frac{\beta_4}{e}.$$

Hence it follows that

$$\frac{u\beta_2 + v\beta_3 + w\beta_4}{e} = \frac{\frac{ua_1b_2+va_2b_1+w(b_2s-2a_2c_2)}{e} + \sqrt{\Delta}}{2} \in C^{-1}\mathfrak{a}_1\mathfrak{a}_2,$$

and therefore we may choose

$$b = B = \frac{ua_1b_2 + va_2b_1 + w(b_2s - 2a_2c_2)}{e} = b_2 + \frac{2a_2}{d}\bigl[v(s-b_2) - wc_2\bigr].$$

If $(a_1,b_1,c_1,a_2,b_2,c_2) = 1$, then $\mathfrak{N}_\Delta(\mathfrak{a}_1\mathfrak{a}_2) = \mathfrak{N}_\Delta(\mathfrak{a}_1)\mathfrak{N}_\Delta(\mathfrak{a}_2)$, since

$$d = \Bigl(a_1, c_1, a_2, c_2, \frac{b_1+b_2}{2}, \frac{b_1-b_2}{2}\Bigr) \Bigm| (a_1,b_1,c_1,a_2,b_2,c_2).$$

If $\mathfrak{a}_i$ is $\mathcal{O}_\Delta$-invertible for some $i \in \{1, 2\}$, then $(a_i,b_i,c_i) = 1$ by Theorem 5.4.2, and therefore $d = 1$. The ideal $\mathfrak{a}_1\mathfrak{a}_2$ is $\mathcal{O}_\Delta$-primitive if and only if $ee_1e_2 = 1$, and this holds if and only if $e_1 = e_2 = e = 1$. □

Exercise 5.4.7. Calculate the product

$$\Bigl[6, \frac{1+\sqrt{97}}{2}\Bigr]\Bigl[18, \frac{5+\sqrt{97}}{2}\Bigr].$$

Exercise 5.4.8. Let Δ be a quadratic discriminant. For $i \in \{1,2\}$, let $\mathfrak{a}_i$ be an ideal of $\mathcal{O}_\Delta$, say

$$\mathfrak{a}_i = \Bigl[a_i, \frac{b_i+\sqrt{\Delta}}{2}\Bigr], \quad \text{where } a_i \in \mathbb{N},\ b_i \in \mathbb{Z} \text{ and } \Bigl(a_1, a_2, \frac{b_1+b_2}{2}\Bigr) = 1.$$

Prove that

$$\mathfrak{a}_1\mathfrak{a}_2 = \Bigl[a_1a_2, \frac{b+\sqrt{\Delta}}{2}\Bigr],$$

where b is any integer satisfying $b \equiv b_i \bmod 2a_i$ for $i \in \{1,2\}$.

5.5. Class groups and class semigroups

We start with the definition of equivalence and proper equivalence of lattices and then we apply these concepts for ideals in quadratic orders. The reader might wonder why we take the trouble to deal with both notions in detail (instead of relegating one of them to the exercises). While equivalence is the natural notion from the ideal-theoretic point of view (see Exercise 5.5.1), proper equivalence yields the connection between ideals and binary quadratic forms which will become apparent in Chapter 6. Thus both notions seem to be important enough to be dealt with in the main text. For an item $\star$ we use the notation $\star^{(+)}$ to mean either $\star$ or $\star^+$.

The main goal of this section is to introduce class semigroups and class groups, to show their finiteness and to parameterize them by means of equivalence classes of quadratic irrationals.

Let K be a quadratic number field. Two lattices $\mathfrak{a}$ and $\mathfrak{b}$ in K are called

- *equivalent*, $\mathfrak{a} \sim \mathfrak{b}$, if $\mathfrak{a} = \lambda\mathfrak{b}$ for some $\lambda \in K^\times$;
- *properly equivalent* or *equivalent in the narrow sense*, $\mathfrak{a} \sim_+ \mathfrak{b}$, if $\mathfrak{a} = \lambda\mathfrak{b}$ for some $\lambda \in K^\times$ such that $\mathcal{N}(\lambda) > 0$.

By definition, proper equivalence implies equivalence. As to the converse, we refer to the subsequent Theorem 5.5.4.

Exercise 5.5.1. Let $\mathfrak{a}$ and $\mathfrak{b}$ be lattices in K and R an order in K such that $R \subset \mathcal{R}(\mathfrak{a}) \cap \mathcal{R}(\mathfrak{b})$ (such an order exists by Exercise 5.1.8). A map $\varphi\colon \mathfrak{a} \to \mathfrak{b}$ is called an *R-isomorphism* if it is a group isomorphism satisfying $\varphi(\lambda\alpha) = \lambda\varphi(\alpha)$ for all $\alpha \in \mathfrak{a}$ and $\lambda \in R$. Prove that $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent if and only if there exists an R-isomorphism $\varphi\colon \mathfrak{a} \to \mathfrak{b}$.

Equivalence and proper equivalence are congruence relations on the multiplicative semigroup $\mathcal{L}(K)$ of all lattices in K, and they are compatible with conjugation. Explicitly, for all $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c} \in \mathcal{L}(K)$ the following assertions hold:

> $\mathfrak{a} \sim_{(+)} \mathfrak{a}$; if $\mathfrak{a} \sim_{(+)} \mathfrak{b}$, then $\mathfrak{b} \sim_{(+)} \mathfrak{a}$, $\mathfrak{a}' \sim_{(+)} \mathfrak{b}'$ and $\mathfrak{a}\mathfrak{c} \sim_{(+)} \mathfrak{b}\mathfrak{c}$; if $\mathfrak{a} \sim_{(+)} \mathfrak{b}$ and $\mathfrak{b} \sim_{(+)} \mathfrak{c}$, then $\mathfrak{a} \sim_{(+)} \mathfrak{c}$.

For a lattice $\mathfrak{a}$ in K, we denote by $[\mathfrak{a}]$ the equivalence class and by $[\mathfrak{a}]^+$ the proper equivalence class of $\mathfrak{a}$. We consider the multiplicative quotient semigroups

$$\mathcal{S}_K = \mathcal{L}(K)/{\sim} = \{[\mathfrak{a}] \mid \mathfrak{a} \in \mathcal{L}(K)\} \quad \text{and} \quad \mathcal{S}_K^+ = \mathcal{L}(K)/{\sim_+} = \{[\mathfrak{a}]^+ \mid \mathfrak{a} \in \mathcal{L}(K)\}$$

built by all (proper) equivalence classes of lattices in K. Multiplication and conjugation of (proper) equivalence classes are defined on representatives. Explicitly, if $\mathfrak{a}$ and $\mathfrak{b}$ are lattices in K, then

$$[\mathfrak{a}]^{(+)}[\mathfrak{b}]^{(+)} = [\mathfrak{a}\mathfrak{b}]^{(+)} \quad \text{and} \quad ([\mathfrak{a}]^{(+)})' = [\mathfrak{a}']^{(+)}\,.$$

We call $\mathcal{S}_K$ the *lattice class semigroup* and $\mathcal{S}_K^+$ the *narrow lattice class semigroup* of K.

Let now Δ be a quadratic discriminant such that $K = \mathbb{Q}(\sqrt{\Delta}\,)$. If two lattices $\mathfrak{a}$ and $\mathfrak{b}$ of K are equivalent, then $\mathcal{R}(\mathfrak{a}) = \mathcal{R}(\mathfrak{b})$. Hence it follows (using the very definition of fractional ideals and Theorem 5.3.5) that $\mathfrak{a}$ is an (invertible) fractional

$\mathcal{O}_\Delta$-ideal if and only if $\mathfrak{b}$ has the same property. This observation causes the following definitions.

> We denote by $\mathcal{S}_\Delta^{(+)}$ the set of all (proper) equivalence classes of fractional $\mathcal{O}_\Delta$-ideals and by $\mathcal{C}_\Delta^{(+)}$ the set of all (proper) equivalence classes of $\mathcal{O}_\Delta$-invertible fractional $\mathcal{O}_\Delta$-ideals.

Since the product of two ($\mathcal{O}_\Delta$-invertible) fractional $\mathcal{O}_\Delta$-ideals is again an ($\mathcal{O}_\Delta$-invertible) fractional $\mathcal{O}_\Delta$-ideal and every $\mathcal{O}_\Delta$-invertible fractional $\mathcal{O}_\Delta$-ideal has an inverse, it follows that $\mathcal{S}_\Delta^{(+)}$ is a submonoid of $\mathcal{S}_K^{(+)}$, and $\mathcal{C}_\Delta^{(+)}$ is a subgroup of $\mathcal{S}_\Delta^{(+)}$. The (narrow) class $[\mathcal{O}_\Delta]^{(+)}$ is the unit element of $\mathcal{S}_\Delta^{(+)}$. It consists of all fractional principal ideals of $\mathcal{O}_\Delta$ (generated by norm-positive elements of K), and it is called the (*narrow*) *principal class*. We call

- $\mathcal{S}_\Delta$ the (*ideal*) *class semigroup*,
- $\mathcal{S}_\Delta^+$ the *narrow* (*ideal*) *class semigroup*,
- $\mathcal{C}_\Delta$ the (*ideal*) *class group* or *Picard group*, and
- $\mathcal{C}_\Delta^+$ the *narrow* (*ideal*) *class group* or the *narrow Picard group* of $\mathcal{O}_\Delta$.

Then elements of $\mathcal{S}_\Delta^{(+)}$ are called (*narrow*) *ideal classes*, and the elements of $\mathcal{C}_\Delta^{(+)}$ are called (*narrow*) *regular ideal classes* of $\mathcal{O}_\Delta$.

If $\mathfrak{a}$ is a fractional $\mathcal{O}_\Delta$-ideal and $\lambda \in K^\times$, then $[\mathfrak{a}] = [\lambda\mathfrak{a}]$, and if $\mathcal{N}(\lambda) > 0$, then even $[\mathfrak{a}]^+ = [\lambda\mathfrak{a}]^+$. Hence every (narrow) ideal class $C \in \mathcal{S}_\Delta^{(+)}$ contains an $\mathcal{O}_\Delta$-primitive ideal, and every (narrow) regular ideal class $C \in \mathcal{C}_\Delta^{(+)}$ contains an $\mathcal{O}_\Delta$-regular ideal. If $C \in \mathcal{C}_\Delta^{(+)}$ is any (narrow) regular ideal class, then every fractional $\mathcal{O}_\Delta$-ideal $\mathfrak{a} \in C$ is $\mathcal{O}_\Delta$-invertible.

If Δ_1 is a quadratic discriminant such that $\mathcal{O}_\Delta \subset \mathcal{O}_{\Delta_1}$, then $\mathcal{S}_{\Delta_1}^{(+)} \subset \mathcal{S}_\Delta^{(+)}$ is a subsemigroup, and $\mathcal{C}_{\Delta_1}^{(+)}$ consists of all (narrow) ideal classes $[\mathfrak{a}] \in \mathcal{S}_\Delta^{(+)}$ such that $\mathcal{R}(\mathfrak{a}) = \mathcal{O}_{\Delta_1}$. Hence $\mathcal{S}_\Delta^{(+)}$ is the (disjoint) union of all groups $\mathcal{C}_{\Delta_1}^{(+)}$ built by quadratic discriminants Δ_1 such that $\mathcal{O}_\Delta \subset \mathcal{O}_{\Delta_1}$.

We pause for a short algebraic consideration of the latter statement in terms of semigroup theory. A (commutative multiplicative) semigroup S is called a *Clifford semigroup* if it is the disjoint union of a family of subgroups. If

$$S = \biguplus_{i \in I} G_i\,, \quad \text{where} \quad G_i \subset S \ \text{ are subgroups with unit elements } \ e_i\,,$$

then $(e_i)_{i\in I}$ is the set of all idempotents of S. The family $(G_i)_{i\in I}$ is called the family of *components* and the family $(e_i)_{i\in I]}$ is called the family of *idempotents* of S. Now we can rephrase our last statement about class semigroups as follows.

Theorem 5.5.2. *Let Δ be a quadratic discriminant and $\mathcal{D}_\Delta$ the set of all quadratic discriminants Δ_1 such that $\mathcal{O}_\Delta \subset \mathcal{O}_{\Delta_1}$. Then $\mathcal{S}_\Delta^{(+)}$ is a Clifford semigroup, $\big(\mathcal{C}_{\Delta_1}^{(+)}\big)_{\Delta_1\in\mathcal{D}_\Delta}$ is the family of components and $\big([\mathcal{O}_{\Delta_1}]^{(+)}\big)_{\Delta_1\in\mathcal{D}(\Delta)}$ is the family of idempotents of $\mathcal{S}_\Delta^{(+)}$.*

Exercise 5.5.3. Let S be a (commutative multiplicative) semigroup. Prove that S is a Clifford semigroup if and only if for every $x \in S$ there exists some $y \in S$ such that $x^2y = x$.

The class group and the narrow class group fit into natural exact sequences of abelian groups as follows. Let Δ be a quadratic discriminant. Recall from the discussion following Theorem 5.3.5 that $\mathcal{F}_\Delta^\times$ denotes the group of all $\mathcal{O}_\Delta$-invertible fractional $\mathcal{O}_\Delta$-ideals and that $\partial\colon K^\times \to \mathcal{F}_\Delta^\times$ was defined by $\partial(a) = a\mathcal{O}_\Delta$. With these data, we obtain an exact sequence for $\mathcal{C}_\Delta$:

$$\mathbf{1} \;\to\; \mathcal{O}_\Delta^\times \;\hookrightarrow\; K^\times \;\xrightarrow{\partial}\; \mathcal{F}_\Delta^\times \;\xrightarrow{[\cdot]}\; \mathcal{C}_\Delta \;\to \mathbf{1}\,.$$

Since $K^+ = \{a \in K \mid \mathcal{N}(a) > 0\}$ is a subgroup of $K^\times$ and $\mathcal{O}_\Delta^{\times +} = \mathcal{O}_\Delta \cap K^+$ is the group of norm-positive units of $\mathcal{O}_\Delta$, we obtain also an exact sequence for $\mathcal{C}_\Delta^+$:

$$\mathbf{1} \;\to\; \mathcal{O}_\Delta^{\times +} \;\hookrightarrow\; K^+ \;\xrightarrow{\partial\,|\,K^+}\; \mathcal{F}_\Delta^\times \;\xrightarrow{[\cdot]^+}\; \mathcal{C}_\Delta^+ \;\to \mathbf{1}\,.$$

In the next theorem we determine the relations between ideal (semi-)groups and narrow ideal (semi-)groups. For positive discriminants Δ, the fundamental unit ε_Δ (and thus Pell's equation) plays an important role. We refer to Theorem 2.2.9 and to Section 5.2 for the properties of ε_Δ.

Theorem 5.5.4. *Let Δ be a quadratic discriminant.*

1. *The* (*narrow*) *ideal class group $\mathcal{C}_\Delta^{(+)}$ is the group of invertible elements of the monoid $\mathcal{S}_\Delta^{(+)}$, and $C' = C^{-1}$ for all $C \in \mathcal{C}_\Delta^{(+)}$.*
2. *Suppose that either $\Delta < 0$, or $\Delta > 0$ and $\mathcal{N}(\varepsilon_\Delta) = -1$. Then two fractional $\mathcal{O}_\Delta$-ideals are properly equivalent if and only if they are equivalent. In particular, $[\mathfrak{a}] = [\mathfrak{a}]^+$ for all fractional $\mathcal{O}_\Delta$-ideals $\mathfrak{a}$, $\mathcal{S}_\Delta = \mathcal{S}_\Delta^+$ and $\mathcal{C}_\Delta = \mathcal{C}_\Delta^+$.*
3. *Suppose that $\Delta > 0$ and $\mathcal{N}(\varepsilon_\Delta) = 1$. Then*
$$[\mathfrak{a}] = [\mathfrak{a}]^+ \cup [\mathfrak{a}\sqrt{\Delta}\,]^+ \quad \textit{for all fractional } \mathcal{O}_\Delta\textit{-ideals } \mathfrak{a},$$
and there is a surjective semigroup homomorphism
$$\theta\colon \mathcal{S}_\Delta^+ \;\to\; \mathcal{S}_\Delta\,, \quad \textit{given by } \theta([\mathfrak{a}]^+) = [\mathfrak{a}] \quad \textit{for all fractional } \mathcal{O}_\Delta\textit{-ideals } \mathfrak{a}.$$
If $\mathfrak{a}$ is an $\mathcal{O}_\Delta$-invertible fractional $\mathcal{O}_\Delta$-ideal, then $[\mathfrak{a}]^+ \neq [\mathfrak{a}\sqrt{\Delta}\,]^+$. The map
$$\theta_0 = \theta\,|\,\mathcal{C}_\Delta^+\colon \mathcal{C}_\Delta^+ \;\to\; \mathcal{C}_\Delta$$
is a surjective group homomorphism, and $\operatorname{Ker}(\theta_0) = \{\,[\mathcal{O}_\Delta]^+,\, [\sqrt{\Delta}\,\mathcal{O}_\Delta]^+\}$. *In particular, $|\mathcal{C}_\Delta^+| = 2|\mathcal{C}_\Delta|$, and every class $C \in \mathcal{C}_\Delta$ splits in the form $C = C_1 \uplus C_2$, where $C_1, C_2 \in \mathcal{C}_\Delta^+$ and $C_2 = C_1[\sqrt{\Delta}\mathcal{O}_\Delta]^+$.*

Proof. We consider the quadratic number field $K = \mathbb{Q}(\sqrt{\Delta}\,)$.

1. Since $\mathcal{C}_\Delta^{(+)}$ is a subgroup of $\mathcal{S}_\Delta^{(+)}$, it suffices to prove that every invertible element of $\mathcal{S}_\Delta^{(+)}$ belongs to $\mathcal{C}_\Delta^{(+)}$. Thus let $C \in (\mathcal{S}_\Delta^{(+)})$ be invertible and $C_1 \in \mathcal{S}_\Delta^{(+)}$ its inverse. Let $\mathfrak{a}$ and $\mathfrak{a}_1$ be fractional $\mathcal{O}_\Delta$-ideals such that $C = [\mathfrak{a}]^{(+)}$ and $C_1 = [\mathfrak{a}_1]^{(+)}$. Then $CC_1 = [\mathfrak{a}\mathfrak{a}_1]^{(+)} = [\mathcal{O}_\Delta]^{(+)}$, and therefore $\mathfrak{a}\mathfrak{a}_1 = \lambda\mathcal{O}_\Delta$ for some $\lambda \in K^\times$. Hence $\mathfrak{a}$ is $\mathcal{O}_\Delta$-invertible and therefore $C = [\mathfrak{a}]^{(+)} \in \mathcal{C}_\Delta^{(+)}$.

If $C \in \mathcal{C}_\Delta^{(+)}$, then $C = [\mathfrak{a}]^{(+)}$ for some $\mathcal{O}_\Delta$-invertible ideal $\mathfrak{a}$ of $\mathcal{O}_\Delta$. By Corollary 5.4.3 we obtain $\mathfrak{a}\mathfrak{a}' = \mathfrak{N}_\Delta(\mathfrak{a})\mathcal{O}_\Delta$, hence $CC' = [\mathfrak{a}\mathfrak{a}']^{(+)} = [\mathcal{O}_\Delta]^{(+)}$, and therefore $C' = C^{-1}$.

2. It suffices to prove that any two equivalent fractional $\mathcal{O}_\Delta$-ideals are properly equivalent. If $\Delta < 0$, then $\mathcal{N}(\lambda) = |\lambda|^2 > 0$ for all $\lambda \in K^\times$, and the assertion follows. Thus suppose that $\Delta > 0$ and $\mathcal{N}(\varepsilon_\Delta) = -1$. Let $\mathfrak{a}$ and $\mathfrak{b}$ be equivalent fractional $\mathcal{O}_\Delta$-ideals and $\lambda \in K^\times$ such that $\mathfrak{b} = \lambda\mathfrak{a}$. Since $\mathfrak{b} = \varepsilon_\Delta\lambda\mathfrak{a}$ and either $\mathcal{N}(\lambda) > 0$ or $\mathcal{N}(\varepsilon_\Delta\lambda) > 0$, it follows that $\mathfrak{a}$ and $\mathfrak{b}$ are properly equivalent.

3. Let $\mathfrak{a}$ be a fractional $\mathcal{O}_\Delta$-ideal and $\mathfrak{b} \in [\mathfrak{a}] \setminus [\mathfrak{a}]^+$. Then $\mathfrak{b} = \lambda\mathfrak{a}$ for some $\lambda \in K^\times$ such that $\mathcal{N}(\lambda) < 0$, but since

$$\mathfrak{b} = \frac{\lambda}{\sqrt{\Delta}}\,(\mathfrak{a}\sqrt{\Delta}) \quad \text{and} \quad \mathcal{N}\Big(\frac{\lambda}{\sqrt{\Delta}}\Big) = \frac{\mathcal{N}(\lambda)}{-\Delta} > 0\,,$$

it follows that $\mathfrak{b} \in [\mathfrak{a}\sqrt{\Delta}\,]^+$. Hence $[\mathfrak{a}] = [\mathfrak{a}]^+ \cup [\mathfrak{a}\sqrt{\Delta}\,]^+$.

By the very definition, $\theta \colon \mathcal{S}_\Delta^+ \to \mathcal{S}_\Delta$ is a surjective semigroup homomorphism, and $\theta_0 = \theta \,|\, \mathcal{C}_\Delta^+ \colon \mathcal{C}_\Delta^+ \to \mathcal{C}_\Delta$ is a surjective group homomorphism. Therefore it suffices to prove that $[\mathfrak{a}]^+ \ne [\mathfrak{a}\sqrt{\Delta}\,]^+$ for every $\mathcal{O}_\Delta$-invertible fractional $\mathcal{O}_\Delta$-ideal. Assume to the contrary that $\mathfrak{a}$ is an $\mathcal{O}_\Delta$-invertible fractional $\mathcal{O}_\Delta$-ideal which is properly equivalent to $\mathfrak{a}\sqrt{\Delta}$. Let $\lambda \in K^\times$ be such that $\mathcal{N}(\lambda) > 0$ and $\mathfrak{a} = \mathfrak{a}\sqrt{\Delta}\,\lambda$. Since $\mathfrak{a}$ is $\mathcal{O}_\Delta$-invertible, it follows that $\mathcal{O}_\Delta = \sqrt{\Delta}\,\lambda\mathcal{O}_\Delta$. Hence we obtain $\sqrt{\Delta}\lambda \in \mathcal{O}_\Delta^\times$ and $\mathcal{N}(\sqrt{\Delta}\lambda) = -\Delta\sqrt{\lambda} < 0$, which is impossible since $\mathcal{N}(\varepsilon_\Delta) = -1$. $\square$

In order to prove the finiteness of the ideal class (semi-)groups we proceed as for quadratic irrationals: We introduce reduced representatives and prove the finiteness of them. Recall from Theorem 5.4.5 that every $\mathcal{O}_\Delta$-regular ideal is of the form $I(\xi)$ for some quadratic irrational ξ of discriminant Δ.

Let Δ be a quadratic discriminant. An ideal $\mathfrak{a}$ of $\mathcal{O}_\Delta$ is called *reduced* if $\mathfrak{a} = I(\xi)$ for some reduced quadratic irrational ξ of discriminant Δ. By Theorem 5.4.5, every reduced ideal of $\mathcal{O}_\Delta$ is $\mathcal{O}_\Delta$-regular.

Theorem 5.5.5. *Let Δ be a quadratic discriminant.*

1. *Let $\mathfrak{a}$ be a reduced ideal of $\mathcal{O}_\Delta$. Then there exists a unique reduced quadratic irrational ξ of discriminant Δ such that $\mathfrak{a} = I(\xi)$, and the ideal $\mathfrak{a}'$ is also reduced.*
2. *Let ξ be a quadratic irrational of type (a,b,c) and discriminant Δ such that $a > 0$. Then $I(\xi)$ is reduced if and only if*
    - *either $\Delta < 0$ and $\xi + n$ lies in the fundamental domain of the modular group for some $n \in \mathbb{Z}$,*
    - *or $\Delta > 0$ and $\xi + \lfloor -\xi' \rfloor > 1$.*

   In particular, the unit ideal $\mathcal{O}_\Delta = I(\omega_\Delta)$ is reduced.

Proof. 1. Let $\mathfrak{a}$ be reduced. Then there exists a reduced quadratic irrational ξ such that $\mathfrak{a} = I(\xi)$. By Theorem 1.3.5.3, the quadratic irrational $\eta = -\xi' + \lfloor \xi \rfloor$ is also reduced, and therefore the ideal $I(\eta) = I(\xi') = \mathfrak{a}'$ is reduced.

To prove the uniqueness of ξ, let ξ and ξ_1 be reduced quadratic irrationals such that $I(\xi) = I(\xi_1)$. Then Theorem 5.4.5.3 implies $\xi_1 = \varepsilon\xi + n$ for some $\varepsilon \in \{\pm 1\}$ and $n \in \mathbb{Z}$.

If $\Delta < 0$, then both ξ and ξ_1 lie in the upper half-plane, hence $\varepsilon = 1$, and since $\Re(\xi), \Re(\xi_1) \in \left(-\frac{1}{2}, \frac{1}{2}\right]$, we obtain $n = 0$ and $\xi = \xi_1$.

If $\Delta > 0$, then $\xi_1' = \varepsilon\xi' + n$, and since $\xi', \xi_1' \in (-1, 0)$, we obtain either $\varepsilon = 1$ and $n = 0$, or $\varepsilon = n = -1$. But in the latter case we get $\xi_1 = -\xi - 1 < 0$, a contradiction. Hence it follows again that $\xi = \xi_1$.

2. Let ξ be a quadratic irrational of type (a, b, c) and discriminant Δ such that $a > 0$. Then $I(\xi)$ is reduced if and only if there exist some $\varepsilon \in \{\pm 1\}$ and $n \in \mathbb{Z}$ such that $\varepsilon\xi + n$ is reduced. Since $-\xi + n$ is not reduced, it follows that $I(\xi)$ is reduced if and only if $\xi + n$ is reduced for some $n \in \mathbb{Z}$. This proves our assertion if $\Delta < 0$.

Thus assume that $\Delta > 0$. If $n \in \mathbb{Z}$ and $\xi + n$ is reduced, then $\xi + n > 1$ and $-1 < \xi' + n < 0$, hence $n < -\xi' < n+1$, and therefore $\xi + \lfloor -\xi' \rfloor > 1 - n + n = 1$. As to the converse, assume that $\xi_1 = \xi + \lfloor -\xi' \rfloor > 1$. Then ξ_1 is a quadratic irrational of discriminant Δ, $\xi_1' = \xi' + \lfloor -\xi' \rfloor$, and $\lfloor -\xi' \rfloor < -\xi' < \lfloor -\xi' \rfloor + 1$ implies $-1 < \xi_1' < 0$. Hence ξ_1 is reduced.

If $\Delta < 0$, then ω_Δ is reduced by Theorem 1.3.2.3. If $\Delta > 0$, then

$$\omega_\Delta + \lfloor -\omega_\Delta' \rfloor = \frac{\sigma_\Delta + \sqrt{\Delta}}{2} + \left\lfloor \frac{-\sigma_\Delta + \sqrt{\Delta}}{2} \right\rfloor > 1\,.$$

Hence it follows in both cases that $I(\omega_\Delta) = [1, \omega_\Delta] = \mathcal{O}_\Delta$ is reduced. □

Exercise 5.5.6. Let $\Delta > 0$ be a quadratic discriminant and $\mathfrak{a}$ an $\mathcal{O}_\Delta$-regular ideal. Prove the following criteria:

1. If $\mathfrak{a}$ is reduced, then $\mathfrak{N}_\Delta(\mathfrak{a}) < \sqrt{\Delta}$.
2. If $2\,\mathfrak{N}_\Delta(\mathfrak{a}) < \sqrt{\Delta}$, then $\mathfrak{a}$ is reduced.

In the following Theorem 5.5.7 we connect the equivalence of ideals with the equivalence of quadratic irrationals and conclude as a first consequence that every (narrow) regular ideal class contains ideals with absolute norm coprime to a given integer. After this, in Theorem 5.5.8, we prove the finiteness results for the class groups and class semigroups based on the corresponding finiteness results for equivalence classes of quadratic irrationals (see Theorem 1.3.10).

Theorem 5.5.7. *Let Δ be a quadratic discriminant and $K = \mathbb{Q}(\sqrt{\Delta})$.*

1. *Let ξ and ξ_1 be quadratic irrationals of discriminant Δ, let ξ be of type (a, b, c) and ξ_1 of type (a_1, b_1, c_1).*
   (a) *If $\lambda \in K^\times$ is such that $I(\xi) = \lambda I(\xi_1)$, then $\xi_1 = A\xi$ for some matrix*

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathsf{GL}_2(\mathbb{Z}) \quad \textit{such that} \quad \lambda = \frac{a}{a_1}(\gamma\xi + \delta)\,.$$

(b) *If* $\xi_1 = A\xi$, *where*

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathsf{GL}_2(\mathbb{Z}) \,, \quad \textit{then} \quad \mathcal{N}(\gamma\xi+\delta) = \frac{a_1}{a}\,\det(A)\,,$$

and

$$I(\xi_1) = \frac{a_1}{a(\gamma\xi+\delta)}\,I(\xi) \ \sim_+ \ \begin{cases} I(\xi) & \textit{if} \quad aa_1\det(A) > 0\,, \\ I(\xi)\sqrt{\Delta} & \textit{if} \quad aa_1\det(A) < 0\,. \end{cases}$$

(c) $I(\xi)$ *and* $I(\xi_1)$ *are equivalent if and only if* ξ *and* ξ_1 *are equivalent.*

(d) *If* $aa_1 > 0$, *then* $I(\xi)$ *and* $I(\xi_1)$ *are properly equivalent if and only if* ξ *and* ξ_1 *are properly equivalent.*

2. *Let* $C \in \mathcal{C}_\Delta^{(+)}$ *be a (narrow) regular ideal class of* $\mathcal{O}_\Delta$.

(a) C *contains a reduced ideal of* $\mathcal{O}_\Delta$, *and only one if* $\Delta < 0$.

(b) *For every positive integer* M, *there exists an* $\mathcal{O}_\Delta$*-regular ideal* $\mathfrak{a}_1 \in C$ *such that* $(\mathfrak{N}_\Delta(\mathfrak{a}_1), M) = 1$ *and* $\mathfrak{N}_\Delta(\mathfrak{a}_1) \ge M$.

PROOF. 1. (a) If $I(\xi) = \lambda I(\xi_1)$, then $[a, a\xi] = [\lambda a_1, \lambda a_1\xi_1]$, and therefore

$$\begin{pmatrix} \lambda a_1\xi_1 \\ \lambda a_1 \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} a\xi \\ a \end{pmatrix} \quad \text{for some matrix} \quad A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathsf{GL}_2(\mathbb{Z})\,,$$

$$\lambda = \frac{\lambda a_1}{a_1} = \frac{a}{a_1}\,(\gamma\xi+\delta) \quad \text{and} \quad \xi_1 = \frac{\lambda a_1\xi_1}{\lambda a_1} = \frac{\alpha a\xi + \beta a}{\gamma a\xi + \delta a} = A\xi\,.$$

(b) If

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \quad \text{and} \quad \xi_1 = A\xi\,, \quad \text{then} \quad \begin{pmatrix} \alpha\xi+\beta \\ \gamma\xi+\delta \end{pmatrix} = A\begin{pmatrix} \xi \\ 1 \end{pmatrix}\,.$$

Hence we obtain

$$I(\xi_1) = a_1\Big[1, \frac{\alpha\xi+\beta}{\gamma\xi+\delta}\Big] = \frac{a_1}{\gamma\xi+\delta}\,[\alpha\xi+\beta, \gamma\xi+\delta] = \frac{a_1}{\gamma\xi+\delta}\,[1,\xi] = \frac{a_1}{a(\gamma\xi+\delta)}\,I(\xi)$$

and

$$\frac{\sqrt{\Delta}}{a_1} = \xi_1 - \xi_1' = \frac{\alpha\xi+\beta}{\gamma\xi+\delta} - \frac{\alpha\xi'+\beta}{\gamma\xi'+\delta} = \frac{(\alpha\delta-\beta\gamma)(\xi-\xi')}{\mathcal{N}(\gamma\xi+\delta)} = \frac{\det(A)}{\mathcal{N}(\gamma\xi+\delta)}\,\frac{\sqrt{\Delta}}{a}\,.$$

Now it follows that

$$\mathcal{N}(\gamma\xi+\delta) = \frac{a_1}{a}\,\det(A)\,, \quad \text{and} \quad I(\xi_1) \sim_+ \begin{cases} I(\xi) & \text{if} \quad aa_1\det(A) > 0\,, \\ I(\xi)\sqrt{\Delta} & \text{if} \quad aa_1\det(A) < 0\,. \end{cases}$$

(c) and (d) are obvious by (a) and (b).

2. Let $C \in \mathcal{C}_\Delta^{(+)}$ be a (narrow) regular ideal class, $\mathfrak{a} \in C$ an $\mathcal{O}_\Delta$-regular ideal and ξ a quadratic irrational of type (a,b,c) such that $a > 0$ and $\mathfrak{a} = I(\xi)$.

(a) CASE 1 : $\Delta < 0$. By Theorem 1.3.2, there exists a unique reduced quadratic irrational ξ_1 which is equivalent to ξ, and therefore $I(\xi_1)$ is a reduced ideal in C. If $\mathfrak{b}$ is any reduced ideal in C, then $\mathfrak{b} = I(\eta)$ for some reduced quadratic irrational η, and $\mathfrak{a} \sim \mathfrak{b}$ implies $\xi \sim \eta$, and consequently $\xi = \eta$ and $\mathfrak{a} = \mathfrak{b}$.

CASE 2 : $\Delta > 0$. By Theorem 1.3.5.1, there exists a reduced quadratic irrational ξ_1 which is properly equivalent to ξ. Then $I(\xi_1)$ is properly equivalent to $I(\xi)$, and $I(\xi_1)$ is a reduced ideal in C.

(b) Let M be a positive integer. By Theorem 2.2.12, there exists a quadratic irrational ξ_1 of type (a_1, b_1, c_1) such that $a_1 \ge M$, $(a_1, M) = 1$, and ξ_1 is properly equivalent to ξ. Then $\mathfrak{a}_1 = I(\xi_1) \in C$ is an $\mathcal{O}_\Delta$-regular ideal, $\mathfrak{N}_\Delta(\mathfrak{a}_1) = a_1 \ge M$, and $(\mathfrak{N}_\Delta(\mathfrak{a}_1), M) = 1$. □

Recall from Section 1.3 that for a quadratic discriminant Δ we denote by $\mathfrak{X}_\Delta$ the (finite) set of all equivalence classes and by $\mathfrak{X}_\Delta^+$ the (finite) set of all proper equivalence classes of quadratic irrationals of discriminant Δ, and we defined the class number h_Δ and the narrow class number h_Δ^+ by

$$h_\Delta = |\mathfrak{X}_\Delta| \quad \text{and} \quad h_\Delta^+ = \begin{cases} h_\Delta & \text{if} \quad \Delta < 0\,, \\ |\mathfrak{X}_\Delta^+| & \text{if} \quad \Delta > 0\,. \end{cases}$$

Theorem 5.5.8. *Let Δ be a quadratic discriminant.*

1. *There is a bijective map*

$$\iota_\Delta \colon \mathfrak{X}_\Delta \ \to \ \mathcal{C}_\Delta$$

such that $\iota_\Delta(X) = [I(\xi)]$ for all equivalence classes $X \in \mathfrak{X}_\Delta$ and all quadratic irrationals $\xi \in X$.

2. *If $\Delta > 0$, then there is a bijective map*

$$\iota_\Delta \colon \mathfrak{X}_\Delta^+ \ \to \ \mathcal{C}_\Delta^+$$

such that $\iota_\Delta(X) = [I(\xi)]^+$ for all proper equivalence classes $X \in \mathfrak{X}_\Delta^+$ and all quadratic irrationals $\xi \in X$ which are of some type (a, b, c) with $a > 0$.

In particular, the class groups $\mathcal{C}_\Delta$ and $\mathcal{C}_\Delta^+$ are finite, $|\mathcal{C}_\Delta| = h_\Delta$ and $|\mathcal{C}_\Delta^+| = h_\Delta^+$.

We call h_Δ the *class number* and h_Δ^+ the *narrow class number* of $\mathcal{O}_\Delta$.

If $\Delta < 0$, then $h_\Delta = h_\Delta^+$. If $\Delta > 0$, then

$$h_\Delta^+ = \frac{2h_\Delta}{(\mathcal{O}_\Delta^\times : \mathcal{O}_\Delta^{\times +})} = \begin{cases} h_\Delta & \textit{if} \ \ \mathcal{N}(\varepsilon_\Delta) = -1\,, \\ 2h_\Delta & \textit{if} \ \ \mathcal{N}(\varepsilon_\Delta) = 1\,, \end{cases}$$

where $\mathcal{O}_\Delta^{\times +} = \{\varepsilon \in \mathcal{O}_\Delta^\times \mid \mathcal{N}(\varepsilon) = 1\}$ denotes the group of norm-positive units.

For an algebraic number field K, we call $h_K = h_{\Delta_K}$ the *class number* and $h_K^+ = h_{\Delta_K}^+$ the *narrow class number* of K.

Proof. 1. Let $\mathbb{X}_\Delta$ denote the set of all quadratic irrationals of discriminant Δ, and define $\tau_\Delta \colon \mathbb{X}_\Delta \to \mathcal{C}_\Delta$ by $\tau_\Delta(\xi) = [I(\xi)]$. Since every regular ideal class of $\mathcal{O}_\Delta$ contains an $\mathcal{O}_\Delta$-regular ideal, the map τ_Δ is surjective. If $\xi, \xi_1 \in \mathbb{X}_\Delta$, then ξ and ξ_1 are equivalent if and only if $[I(\xi)] = [I(\xi_1)] \in \mathcal{C}_\Delta$. Hence τ_Δ induces a bijection $\iota_\Delta \colon \mathfrak{X}_\Delta \to \mathcal{C}_\Delta$ as asserted.

2. Let $\mathbb{X}_\Delta^+$ denote the set of all quadratic irrationals of discriminant Δ and some type (a, b, c) such that $a > 0$. Then $\mathfrak{X}_\Delta^+ = \mathbb{X}_\Delta^+/\!\sim_+$ (since every quadratic irrational

is equivalent to a reduced quadratic irrational and reduced quadratic irrationals are of type (a,b,c) with $a>0$). We define $\tau_\Delta\colon \mathbb{X}_\Delta^+ \to \mathcal{C}_\Delta^+$ by $\tau_\Delta(\xi)=[I(\xi)]^+$. Every regular ideal class of $\mathcal{O}_\Delta$ contains an ideal of the form $I(\xi)$, where $\xi\in\mathbb{X}_\Delta^+$, and if $\xi,\,\xi_1\in\mathbb{X}_\Delta^+$, then ξ and ξ_1 are properly equivalent if and only if $[I(\xi)]^+=[I(\xi_1)]^+$. Hence τ_Δ induces a bijection $\iota_\Delta\colon \mathfrak{X}_\Delta^+\to\mathcal{C}_\Delta^+$ as asserted.

As to the last statement, observe that $\mathcal{C}_\Delta=\mathcal{C}_\Delta^+$ if $\Delta<0$. If $\Delta>0$, we refer to Theorem 1.3.10 and note that Pell's minus equation has integral solutions if and only if $\mathcal{N}(\varepsilon_\Delta)=-1$. Moreover,

$$(\mathcal{O}_\Delta^\times{:}\mathcal{O}_\Delta^{\times+})=\begin{cases}2 & \text{if Pell's minus equation has integral solutions,}\\ 1 & \text{otherwise.}\quad\square\end{cases}$$

Corollary 5.5.9. *Let Δ be a quadratic discriminant. Then the ideal class semigroup $\mathcal{S}_\Delta$ and the narrow ideal class semigroup $\mathcal{S}_\Delta^+$ are finite monoids.*

PROOF. $\mathcal{S}_\Delta^{(+)}$ is the union of finitely many finite groups $\mathcal{C}_{\Delta_1}^{(+)}$ and thus finite. □

Theorem 5.5.10. *Let Δ be a quadratic discriminant. Then $h_\Delta=1$ if and only if every $\mathcal{O}_\Delta$-invertible (fractional) $\mathcal{O}_\Delta$-ideal is principal.*

PROOF. If $h_\Delta=1$, then $\mathcal{C}_\Delta=\{[\mathcal{O}_\Delta]\}$, and thus every $\mathcal{O}_\Delta$-invertible fractional ideal is principal. Conversely, assume that every $\mathcal{O}_\Delta$-invertible ideal is principal. Since every proper ideal class of $\mathcal{O}_\Delta$ contains an $\mathcal{O}_\Delta$-regular (and thus $\mathcal{O}_\Delta$-invertible) ideal, it follows that $\mathcal{C}_\Delta=\{[\mathcal{O}_\Delta]\}$ and $h_\Delta=1$. □

If Δ is a quadratic discriminant such that $\mathcal{O}_\Delta$ is a principal ideal domain, then $\mathcal{O}_\Delta$ is factorial, Δ is a fundamental discriminant and $h_\Delta=1$ by Theorem 5.5.10. Conversely, if $h_\Delta=1$, then $\mathcal{O}_\Delta$ need not be a principal ideal domain ($\Delta=-12$ and $\Delta=20$ are counterexamples). Using multiplicative ideal theory, we shall prove in Theorem 5.8.6 that $\mathcal{O}_\Delta$ is factorial if and only if it is a principal ideal domain.

5.6. Ambiguous ideals and ideal classes

In this section we investigate the elements of order 2 in the (narrow) ideal class group $\mathcal{C}_\Delta^{(+)}$ for a quadratic discriminant Δ. While in general the structure of ideal class groups is unknown, we have precise information on the elements of order 2. They are closely connected with Gauss' theory of genera (see Section 6).

Let Δ be a quadratic discriminant. For an investigation of the elements of order 2 in the (narrow) class group, the following definitions are basic:

- An ideal $\mathfrak{a}$ of $\mathcal{O}_\Delta$ is called *ambiguous* if $\mathfrak{a}=\mathfrak{a}'$.
- A (narrow) regular ideal class $C\in\mathcal{C}_\Delta^{(+)}$ is called *ambiguous* if $C=C'$.

Theorem 5.6.1. *Let Δ be a quadratic discriminant.*

1. *An $\mathcal{O}_\Delta$-invertible ideal $\mathfrak{a}$ of $\mathcal{O}_\Delta$ is ambiguous if and only if $\mathfrak{a}^2=\mathfrak{N}_\Delta(\mathfrak{a})\mathcal{O}_\Delta$.*
2. *A (narrow) regular ideal class $C\in\mathcal{C}_\Delta^{(+)}$ is ambiguous if and only if $C^2=[\mathcal{O}_\Delta]^{(+)}$.*

PROOF. 1. If $\mathfrak{a}$ is an $\mathcal{O}_\Delta$-invertible ideal of $\mathcal{O}_\Delta$, then $\mathfrak{a}\mathfrak{a}' = \mathfrak{N}_\Delta(\mathfrak{a})\mathcal{O}_\Delta$ by Corollary 5.4.3.1, and therefore $\mathfrak{a} = \mathfrak{a}'$ if and only if $\mathfrak{a}^2 = \mathfrak{N}_\Delta(\mathfrak{a})\mathcal{O}_\Delta$.

2. If $C \in \mathcal{C}_\Delta^{(+)}$, then $CC' = [\mathcal{O}_\Delta]^{(+)}$ by Theorem 5.5.4.1, and consequently $C^2 = [\mathcal{O}_\Delta]^{(+)}$ if and only if $C = C'$. □

If $\mathfrak{a}$ is an $\mathcal{O}_\Delta$-invertible ambiguous ideal of $\mathcal{O}_\Delta$, then its (narrow) ideal class $C = [\mathfrak{a}]^{(+)} \in \mathcal{C}_\Delta^{(+)}$ is ambiguous since $C' = [\mathfrak{a}']^{(+)}$, and if $e \in \mathbb{N}$ is such that $e^{-1}\mathfrak{a}$ is $\mathcal{O}_\Delta$-primitive, then $e^{-1}\mathfrak{a}$ is an $\mathcal{O}_\Delta$-regular ambiguous ideal, and $C = [e^{-1}\mathfrak{a}]^{(+)}$. Hence every regular ideal class of $\mathcal{O}_\Delta$ which contains an ambiguous ideal also contains an $\mathcal{O}_\Delta$-regular ambiguous ideal. However, there may exist ambiguous ideal classes without ambiguous ideals. The precise connection is disclosed in the following Theorem 5.6.2.

Theorem 5.6.2. *Let Δ be a quadratic discriminant.*

1. *Every narrow ambiguous class $C \in \mathcal{C}_\Delta^+$ contains an $\mathcal{O}_\Delta$-regular ambiguous ideal.*
2. *A regular ideal class $C \in \mathcal{C}_\Delta$ is an ambiguous class without an ambiguous ideal if and only if $C = C_1 \uplus C_2$, where $C_1, C_2 \in \mathcal{C}_\Delta^+$ are narrow regular ideal classes and $C_1^2 = C_2^2 = [\sqrt{\Delta}\mathcal{O}_\Delta]^+ \ne [\mathcal{O}_\Delta]^+$. If this is the case, then*

$$\Delta > 0\,, \quad \mathcal{N}(\varepsilon_\Delta) = 1\,, \quad C_2 = C_1[\sqrt{\Delta}\mathcal{O}_\Delta]^+ \quad \text{and} \quad C_1^4 = C_2^4 = [\mathcal{O}_\Delta]^+\,.$$

   In particular, if either $\Delta < 0$, or $\Delta > 0$ and $\mathcal{N}(\varepsilon_\Delta) = -1$, then every ambiguous class $C \in \mathcal{C}_\Delta$ contains an $\mathcal{O}_\Delta$-regular ambiguous ideal.
3. *The product of two ambiguous classes without an ambiguous ideal contains an ambiguous ideal.*

PROOF. 1. Let $C \in \mathcal{C}_\Delta^+$ be a narrow ambiguous class and $\mathfrak{a} \in C$ an $\mathcal{O}_\Delta$-invertible ideal. Then $\mathfrak{a}' \in C' = C$, hence $\mathfrak{a}'$ and $\mathfrak{a}$ are properly equivalent, say $\mathfrak{a}' = \lambda\mathfrak{a}$ for some $\lambda \in K^\times$ such that $\mathcal{N}(\lambda) > 0$. We may assume that $\mathcal{T}(\lambda) = \lambda + \lambda' > 0$ (otherwise we replace λ by $-\lambda$). Since $\mathfrak{N}_\Delta(\mathfrak{a}) = \mathfrak{N}_\Delta(\mathfrak{a}') = \mathcal{N}(\lambda)\mathfrak{N}_\Delta(\mathfrak{a})$, we obtain $\mathcal{N}(\lambda) = \lambda\lambda' = 1$. It follows that $\alpha = 1 + \lambda \in K^\times$, $\alpha' = 1 + \lambda' = 1 + \lambda^{-1} = \alpha\lambda^{-1}$, $(\alpha\mathfrak{a})' = \alpha'\mathfrak{a}' = \alpha'\lambda\mathfrak{a} = \alpha\mathfrak{a}$ and $\mathcal{N}(\alpha) = \alpha\alpha' = 2 + \lambda + \lambda' = 2 + \mathcal{T}(\lambda) > 0$. Hence $\alpha\mathfrak{a}$ is properly equivalent to $\mathfrak{a}$, $\alpha\mathfrak{a} \in C$ is an $\mathcal{O}_\Delta$-invertible ambiguous ideal, and therefore C contains an $\mathcal{O}_\Delta$-regular ambiguous ideal.

2. Let $C \in \mathcal{C}_\Delta$ be an ambiguous class without an ambiguous ideal. By 1., C is not a narrow ideal class, and therefore C splits into two distinct narrow classes C_1 and C_2, which (again by 1.) are not ambiguous. For $i \in \{1,2\}$, $C_i^2 \ne [\mathcal{O}_\Delta]^+$, but $C_i \subset C$ implies $C_i^2 \subset C^2 = [\mathcal{O}_\Delta] = [\mathcal{O}_\Delta]^+ \cup [\sqrt{\Delta}\mathcal{O}_\Delta]^+$, and therefore $C_i^2 = [\sqrt{\Delta}\mathcal{O}_\Delta]^+$ and $C_i^4 = [\mathcal{O}_\Delta]^+$. In particular, it follows by Theorem 5.5.4 that $\Delta > 0$ and $\mathcal{N}(\varepsilon_\Delta) = 1$.

Assume now that $C \in \mathcal{C}_\Delta$ splits into two distinct narrow classes $C_1, C_2 \in \mathcal{C}_\Delta^+$ such that $C_1^2 = C_2^2 = [\sqrt{\Delta}\mathcal{O}_\Delta]^+ \ne [\mathcal{O}_\Delta]^+$. Then C_1 and C_2 are not ambiguous, and thus there is no ambiguous ideal in $C_1 \cup C_2 = C$. However, C is an ambiguous class, since $C^2 = [\sqrt{\Delta}\mathcal{O}_\Delta] = [\mathcal{O}_\Delta]$.

3. Let C_1, $C_2 \in \mathcal{C}_\Delta$ be ambiguous classes without an ambiguous ideal. By 2., there exist narrow classes C_1^*, $C_2^* \in \mathcal{C}_\Delta^+$ such that $C_i^* \subset C_i$ and $C_i^{*2} = [\sqrt{\Delta}\mathcal{O}_\Delta]^+$ for $i \in \{1,2\}$. Since $(C_1^*C_2^*)^2 = ([\sqrt{\Delta}\mathcal{O}_\Delta]^+)^2 = [\mathcal{O}_\Delta]^+$, it follows that $C_1^*C_2^*$ is a narrow ambiguous class, and by 1. there exists an ambiguous ideal $\mathfrak{a}$ of $\mathcal{O}_\Delta$ such that $\mathfrak{a} \in C_1^*C_2^* \subset C_1C_2$. $\square$

Exercise 5.6.3. Let $\mathfrak{a} = [9, 15+\sqrt{306}]$. Show that $\mathcal{R}(\mathfrak{a}) = \mathcal{O}_{136}$, and $[\mathfrak{a}] \in \mathcal{C}_{136}$ is an ambiguous class without an ambiguous ideal.

Finally, in Theorem 5.6.11 we shall count the number of ambiguous ideal classes. Before however, we provide an explicit description of all $\mathcal{O}_\Delta$-regular ideals and the equivalence relations between them. This is done by the following two theorems and will enable us to count the ambiguous classes which contain an ambiguous ideal. In order to investigate ambiguous classes without ambiguous ideals we shall (following [**40**]) introduce symmetric ideals and study their interrelation with ambiguous classes in Theorem 5.6.8.

Theorem 5.6.4 (Classification of ambiguous ideals). *Let Δ be a quadratic discriminant.*

A. *An $\mathcal{O}_\Delta$-regular ideal $\mathfrak{a}$ is ambiguous if and only if it is of one of the following two types*:

$$\text{(I)} \qquad \mathfrak{a} = \Big[a, \frac{\sqrt{\Delta}}{2}\Big], \quad \textit{where} \quad a \in \mathbb{N}, \ \ 4a \mid \Delta \quad \textit{and} \quad \Big(a, \frac{\Delta}{4a}\Big) = 1\,;$$

$$\text{(II)} \quad \mathfrak{a} = \Big[a, \frac{a+\sqrt{\Delta}}{2}\Big], \quad \textit{where} \quad a \in \mathbb{N}, \ \ 4a \mid a^2-\Delta \quad \textit{and} \quad \Big(a, \frac{a^2-\Delta}{4a}\Big) = 1\,.$$

More precisely, the following assertions hold:

(a) *If $\Delta \equiv 1 \bmod 4$, then there are no $\mathcal{O}_\Delta$-regular ambiguous ideals of type* (I), *and those of type* (II) *are of the form*

$$\mathfrak{a} = \Big[a, \frac{a+\sqrt{\Delta}}{2}\Big], \quad \textit{where} \quad a \in \mathbb{N}, \ \ a \mid \Delta \quad \textit{and} \quad \Big(a, \frac{\Delta}{a}\Big) = 1\,.$$

(b) *If $\Delta = 4D$ with $D \in \mathbb{Z}$, then the $\mathcal{O}_\Delta$-regular ambiguous ideals of type* (I) *are of the form*

$$\mathfrak{a} = [a, \sqrt{D}\,], \quad \textit{where} \quad a \in \mathbb{N}, \ \ a \mid D \quad \textit{and} \quad \Big(a, \frac{D}{a}\Big) = 1\,.$$

(c) *If $\Delta = 4D$ with $D \in \mathbb{Z}$ and $D \equiv 3 \bmod 4$, then the $\mathcal{O}_\Delta$-regular ambiguous ideals of type* (II) *are of the form*

$$\mathfrak{a} = [2a, a+\sqrt{D}\,], \quad \textit{where} \quad a \in \mathbb{N}, \ \ a \mid D \quad \textit{and} \quad \Big(a, \frac{D}{a}\Big) = 1\,.$$

(d) *If* $\Delta = 4D$ *with* $D \in \mathbb{Z}$ *and* $8 \,|\, D$, *then the* $\mathcal{O}_\Delta$*-regular ambiguous ideals of type* (II) *are of the form*

$$\mathfrak{a} = [4a, 2a + \sqrt{D}\,], \quad \text{where} \quad a \in \mathbb{N}, \;\; 4a \,|\, D \quad \text{and} \quad \Big(a, \frac{D}{4a}\Big) = 1\,.$$

(e) *If* $\Delta = 4D$ *with* $D \in \mathbb{Z}$ *such that* $8 \nmid D$ *or* $D \not\equiv 3 \bmod 4$, *then there are no* $\mathcal{O}_\Delta$*-regular ambiguous ideals of type* (II).

B. *If*

$$\mu(\Delta) = \begin{cases} r & \text{if} \quad \Delta \equiv 1 \bmod 4 \quad \text{or} \quad \Delta \equiv 4 \bmod 16\,, \\ r+1 & \text{if} \quad \Delta \equiv 8 \text{ or } 12 \bmod 16 \quad \text{or} \quad \Delta \equiv 16 \bmod 32\,, \\ r+2 & \text{if} \quad \Delta \equiv 0 \bmod 32\,, \end{cases}$$

then $2^{\mu(\Delta)}$ *is the number of* $\mathcal{O}_\Delta$*-regular ambiguous ideals in* $\mathcal{O}_\Delta$.

Proof. Let $\Delta = \varepsilon 2^e p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$, where $\varepsilon \in \{\pm 1\}$, $r, e \in \mathbb{N}_0$, $e_1, \ldots, e_r \in \mathbb{N}$ and $p_1, \ldots, p_r$ are distinct odd primes. For $i \in [1, r]$, set $q_i = p_i^{e_i}$. Then $\Delta = 2^e d$, where $d = \varepsilon q_1 \cdot \ldots \cdot q_r$. We denote by $\nu_{(\mathrm{I})}(\Delta)$ resp. $\nu_{(\mathrm{II})}(\Delta)$ the number of $\mathcal{O}_\Delta$-regular ambiguous ideals of $\mathcal{O}_\Delta$ of type (I) resp. (II) and we set $\nu(\Delta) = \nu_{(\mathrm{I})}(\Delta) + \nu_{(\mathrm{II})}(\Delta)$.

Let $\mathfrak{a}$ be an $\mathcal{O}_\Delta$-regular ideal of $\mathcal{O}_\Delta$. By Theorem 5.4.2 there exist uniquely determined integers $a \in \mathbb{N}$ and $b \in [0, 2a-1]$ such that

$$4a \,|\, b^2 - \Delta\,, \quad \Big(a, b, \frac{b^2 - \Delta}{4a}\Big) = 1 \quad \text{and} \quad \mathfrak{a} = \Big[a, \frac{b + \sqrt{\Delta}}{2}\Big]\,.$$

By definition, $\mathfrak{a}$ is ambiguous if and only if $\mathfrak{a} = \mathfrak{a}'$, which is equivalent to

$$\Big[a, \frac{b + \sqrt{\Delta}}{2}\Big] = \Big[a, \frac{-b + \sqrt{\Delta}}{2}\Big]\,.$$

This holds if and only if $b \equiv -b \bmod 2a$, that is, if and only if either $b = 0$ or $b = a$. If $b = 0$, then $\mathfrak{a}$ is of type (I), and if $b = a$, then $\mathfrak{a}$ is of type (II). Now we consider the various possibilities for Δ.

CASE 1: $\Delta \equiv 1 \bmod 4$. Apparently, there are no $\mathcal{O}_\Delta$-regular ambiguous ideals of type (I). If $a \in \mathbb{N}$, then $4a \,|\, a^2 - \Delta$ if and only if $a \,|\, \Delta$, and then

$$\Big(a, \frac{a^2 - \Delta}{4a}\Big) = \Big(a, \frac{a^2 - \Delta}{a}\Big) = \Big(a, \frac{\Delta}{a}\Big)\,.$$

Hence it follows that

$$\begin{aligned} \nu(\Delta) = \nu_{(\mathrm{II})}(\Delta) = \;& \Big|\Big\{a \in \mathbb{N} \;\Big|\; a \,|\, \Delta\,,\; \gcd\Big(a, \frac{\Delta}{a}\Big) = 1\Big\}\Big| \;=\; \Big|\Big\{\prod_{j \in J} q_j \;\Big|\; J \subset [1, r]\Big\}\Big| \\ = \;& 2^r = 2^{\mu(\Delta)}\,. \end{aligned}$$

CASE 2: $\Delta = 4D \equiv 4 \bmod 8$. We first consider ideals of type (I). If $a \in \mathbb{N}$, then $4a \,|\, \Delta$ if and only if $a \,|\, D$, and then

$$\Big(a, \frac{\Delta}{4a}\Big) = \Big(a, \frac{D}{a}\Big)\,.$$

Hence we obtain

$$\nu_{(\mathrm{I})}(\Delta) = \Bigl|\Bigl\{a \in \mathbb{N} \Bigm| a \mid D\,,\ \gcd\Bigl(a, \frac{D}{a}\Bigr) = 1\Bigr\}\Bigr| = \Bigl|\Bigl\{\prod_{j\in J} q_j \Bigm| J \subset [1,r]\Bigr\}\Bigr| = 2^r\,.$$

Now we investigate ideals of type (II). If $a \in \mathbb{N}$, then $4a \mid a^2 - \Delta$ if and only if $a = 2a_1$ for some $a_1 \in \mathbb{N}$ such that $2 \nmid a_1$ and $2a_1 \mid a_1^2 - D$ (which is equivalent to $a_1 \mid D$). Therefore $4a \mid a^2 - \Delta$ holds if and only if $a = 2a_1$, where $a_1 \in \mathbb{N}$, $a_1 \mid D$, and we set

$$g = \Bigl(a, \frac{a^2 - \Delta}{4a}\Bigr) = \Bigl(2a_1, \frac{a_1^2 - D}{2a_1}\Bigr)\,.$$

CASE 2a: $\Delta = 4D \equiv 4 \bmod 16$, $D \equiv 1 \bmod 4$. Then $a_1^2 - D \equiv 0 \bmod 4$, and since $2 \nmid a_1$, it follows that $2 \mid g$. Hence there are no $\mathcal{O}_\Delta$-regular ambiguous ideals of type (II), and we obtain $\nu(\Delta) = \nu_{(\mathrm{I})}(\Delta) = 2^r = 2^{\mu(\Delta)}$.

CASE 2b: $\Delta = 4D \equiv 12 \bmod 16$, $D \equiv 3 \bmod 4$. Then $a_1^2 - D \equiv 2 \bmod 4$,

$$g = \Bigl(2a_1, \frac{a_1^2 - D}{2a_1}\Bigr) = \Bigl(a_1, \frac{a_1^2 - D}{a_1}\Bigr) = \Bigl(a_1, \frac{D}{a_1}\Bigr)\,,$$

and therefore

$$\nu_{(\mathrm{II})}(\Delta) = \Bigl|\Bigl\{a_1 \in \mathbb{N} \Bigm| a_1 \mid D\,,\ \gcd\Bigl(a_1, \frac{D}{a_1}\Bigr) = 1\Bigr\}\Bigr| = \Bigl|\Bigl\{\prod_{j\in J} q_j \Bigm| J \subset [1,r]\Bigr\}\Bigr| = 2^r\,.$$

Hence we obtain $\nu(\Delta) = \nu_{(\mathrm{I})}(\Delta) + \nu_{(\mathrm{II})}(\Delta) = 2^r + 2^r = 2^{r+1} = 2^{\mu(\Delta)}$.

CASE 3: $\Delta = 4D \equiv 0 \bmod 8$, $e \ge 3$, $D = 2^{e-2}d$. We first consider ideals of type (I). If $a \in \mathbb{N}$, then $4a \mid \Delta$ holds if and only if $a \mid D$, and then

$$\Bigl(a, \frac{\Delta}{4a}\Bigr) = \Bigl(a, \frac{D}{a}\Bigr)\,.$$

We set $q_0 = 2^{e-2}$ and obtain

$$\nu_{(\mathrm{I})}(\Delta) = \Bigl|\Bigl\{a \in \mathbb{N} \Bigm| a \mid D\,,\ \Bigl(a, \frac{D}{a}\Bigr) = 1\Bigr\}\Bigr| = \Bigl|\Bigl\{\prod_{j\in J} q_j \Bigm| J \subset [0,r]\Bigr\}\Bigr| = 2^{r+1}\,.$$

Now we investigate ideals of type (II). If $a \in \mathbb{N}$, then $4a \mid a^2 - \Delta$ if and only if $a = 4a_2$ for some $a_2 \in \mathbb{N}$ and $a \mid D$.

CASE 3a: $\Delta \equiv 8 \bmod 16$, $e = 3$, $4 \nmid D$. Then $\nu_{(\mathrm{II})}(\Delta) = 0$, and therefore $\nu(\Delta) = \nu_{(\mathrm{I})}(\Delta) = 2^{r+1} = 2^{\mu(\Delta)}$.

CASE 3b: $\Delta \equiv 0 \bmod 16$, $e \ge 4$, $4 \mid D$. If $a = 4a_2 \mid D$, then

$$g = \Bigl(a, \frac{a^2 - \Delta}{4a}\Bigr) = \Bigl(4a_2, \frac{16a_2^2 - 4D}{16a_2}\Bigr) = \Bigl(4a_2,\, a_2 - \frac{D}{4a_2}\Bigr)\,.$$

CASE 3b$'$: $\Delta \equiv 16 \bmod 32$, $e = 4$, $D \equiv 4 \bmod 8$. If $a = 4a_2 \mid D$, then $2 \nmid a_2$, hence $2 \mid g$, $\nu_{(\mathrm{II})}(\Delta) = 0$, and $\nu(\Delta) = \nu_{(\mathrm{I})}(\Delta) = 2^{r+1} = 2^{\mu(\Delta)}$.

CASE 3b$''$: $\Delta \equiv 0 \bmod 32$, $e \ge 5$, $D = 2^{e-2}d$. If $a = 4a_2 \mid D$, then $a_2 \mid 2^{e-4}d$, hence $a_2 = 2^\lambda c$, where $\lambda \in [0, e-4]$, $c \in \mathbb{N}$ and $c \mid d$. We obtain

$$g = \Bigl(4a_2,\, a_2 - \frac{2^{e-4}d}{a_2}\Bigr) = \Bigl(2^{\lambda+2}c, 2^\lambda c - 2^{e-4-\lambda}\,\frac{d}{c}\Bigr)\,,$$

and $g=1$ if and only if

$$\lambda \in \{0, e-4\} \quad \text{and} \quad \Bigl(c, \frac{d}{c}\Bigr) = 1\,,$$

which is equivalent to

$$\Bigl(a_2, \frac{D}{4a_2}\Bigr) = \Bigl(2^\lambda c,\, 2^{e-4-\lambda}\,\frac{d}{c}\Bigr) = 1\,.$$

Consequently, $g=1$ and $4a \,|\, a^2-\Delta$ holds if and only if there is a subset $J \subset [1,r]$ such that

$$\text{either} \quad a = 4\prod_{j\in J} q_j \quad \text{or} \quad a = 2^{e-2}\prod_{j\in J} q_j\,.$$

Hence $\nu_{(\mathrm{II})}(\Delta) = 2^{r+1}$, and $\nu(\Delta) = \nu_{(\mathrm{I})}(\Delta) + \nu_{(\mathrm{II})}(\Delta) = 2^{r+2} = 2^{\mu(\Delta)}$. □

Exercise 5.6.5. Let Δ be a fundamental discriminant and D the product of all primes dividing Δ, that means,

$$D = \begin{cases} D_0 & \text{if} \quad D_0 \not\equiv 3 \mod 4\,, \\ 2D_0 & \text{if} \quad D_0 \equiv 3 \mod 4\,, \end{cases}$$

where D_0 denotes the squarefree kernel of Δ. Let $\mathfrak a$ be a non-zero ideal of $\mathcal O_\Delta$. Prove the following assertions:

a) If $\mathfrak a$ is primitive and ambiguous, then $\mathfrak N_\Delta(\mathfrak a) \,|\, D$.

b) If $\mathfrak N_\Delta(\mathfrak a) \,|\, D$, then $\mathfrak a$ is ambiguous.

Both assertions fail if Δ is not a fundamental discriminant.

Exercise 5.6.6. Let Δ be a quadratic discriminant.

a) Suppose that $\varepsilon \in \mathcal O_\Delta^\times$ and $\mathcal N(\varepsilon_\Delta) = 1$. Prove that $(1+\varepsilon)\mathcal O_\Delta$ is an ambiguous ideal of $\mathcal O_\Delta$.

b) Let $p \equiv 1 \mod 4$ be a prime discriminant and $\mathfrak a$ a non-zero ideal of $\mathcal O_p$. Prove that $\mathfrak a$ is ambiguous if and only if $\mathfrak a = c\sqrt{p}^{\,\delta}\mathcal O_p$ for some $c \in \mathbb N$ and $\delta \in \{0,1\}$. Conclude (using **a)**) that $\mathcal N(\varepsilon_p) = -1$.

The following Theorem 5.6.7 supplements and refines Theorem 5.6.4.

Theorem 5.6.7. *Let Δ be a quadratic discriminant such that $\Delta \notin \{-3,-4\}$.*

1. *Suppose that $\Delta = 4D$ and $D = \varepsilon dd^*$, where $\varepsilon = \operatorname{sgn}(\Delta)$, $d, d^* \in \mathbb N$, $d \le d^*$ and $(d,d^*)=1$. Then $d<d^*$, the ideals*

$$\mathfrak a = [d, \sqrt D\,] \quad \textit{and} \quad \mathfrak a^* = [d^*, \sqrt D\,] = d^{-1}\sqrt D\,\mathfrak a$$

are distinct $\mathcal O_\Delta$-regular ambiguous ideals, and all $\mathcal O_\Delta$-regular ambiguous ideals of type (I) *arise in this way. If $\mathfrak a$ and $\mathfrak a^*$ are as above, then the following assertions hold:*

- *$\mathfrak a \sim \mathfrak a^*$, and if $\Delta > 0$, then $\mathfrak a \sim_+ \mathfrak a^*$ if and only if $\mathcal N(\varepsilon_\Delta) = -1$.*
- *$\mathfrak a$ is reduced and $\mathfrak a^*$ is not reduced.*

2. *Suppose that* $\mathcal{O}_\Delta$ *contains ambiguous ideals of type* (II), *and assume that* $\Delta = \varepsilon dd^*$, *where* $\varepsilon = \operatorname{sgn}(\Delta)$, $d,\, d^* \in \mathbb{N}$, $d \le d^*$, *and* $d - \varepsilon d^* = 4c$ *for some* $c \in \mathbb{Z}$ *such that* $(c,d) = 1$. *Then* $d < d^*$, *the ideals*

$$\mathfrak{a} = \Bigl[d, \frac{d+\sqrt{\Delta}}{2}\Bigr] \quad \textit{and} \quad \mathfrak{a}^* = \Bigl[d^*, \frac{d^*+\sqrt{\Delta}}{2}\Bigr] = d^{-1}\sqrt{\Delta}\,\mathfrak{a}$$

are distinct $\mathcal{O}_\Delta$*-regular ambiguous ideals, and all* $\mathcal{O}_\Delta$*-regular ambiguous ideals of type* (II) *arise in this way. If* $\mathfrak{a}$ *and* $\mathfrak{a}^*$ *are as above, then the following assertions hold:*

- $\mathfrak{a} \sim \mathfrak{a}^*$, *and if* $\Delta > 0$, *then* $\mathfrak{a} \sim_+ \mathfrak{a}^*$ *if and only if* $\mathcal{N}(\varepsilon_\Delta) = -1$.
- *If* $\Delta > 0$, *then* $\mathfrak{a}$ *is reduced and* $\mathfrak{a}^*$ *is not reduced.*
- *If* $\Delta < 0$, *then* $\mathfrak{a}$ *is also equivalent to the* $\mathcal{O}_\Delta$*-regular ideal*

$$\widetilde{\mathfrak{a}} = \Bigl[c, \frac{-d+\sqrt{\Delta}}{2}\Bigr],$$

exactly one of the ideals $\mathfrak{a}$ *and* $\widetilde{\mathfrak{a}}$ *is reduced, and* $\mathfrak{a}^*$ *is not reduced.*

3. A pair $(\mathfrak{a}, \mathfrak{a}^*)$ of $\mathcal{O}_\Delta$-regular ideals as in 1. or 2. is called an *ambiguous pair* in $\mathcal{O}_\Delta$. *Every* $\mathcal{O}_\Delta$*-regular ambiguous ideal occurs in exactly one ambiguous pair. If* $\Delta < 0$ *and* $(\mathfrak{a}, \mathfrak{a}^*)$, $(\mathfrak{a}_1, \mathfrak{a}_1^*)$ *are ambiguous pairs of type* (II), *then* $\widetilde{\mathfrak{a}} = \widetilde{\mathfrak{a}}_1$ *implies* $\mathfrak{a} = \mathfrak{a}_1$.

PROOF. 1. Since $\Delta = \varepsilon dd^* \ne -4$ and $(d, d^*) = 1$, we obtain $d \ne d^*$. Apparently, $\mathfrak{a}$ and $\mathfrak{a}^*$ are distinct $\mathcal{O}_\Delta$-regular ambiguous ideals of type (I), and all $\mathcal{O}_\Delta$-regular ambiguous ideals of type (I) in $\mathcal{O}_\Delta$ arise in this way.

Since $\mathfrak{a}\sqrt{D} = [d\sqrt{D}, D] = d[d^*, \sqrt{D}] = d\mathfrak{a}^*$, we obtain $\mathfrak{a}^* = d^{-1}\sqrt{D}\mathfrak{a} \sim \mathfrak{a}$. If $\Delta > 0$, then Theorem 5.5.4 implies that $\mathfrak{a} \sim_+ \mathfrak{a}^*$ if and only if $\mathcal{N}(\varepsilon_\Delta) = -1$. It remains to prove that $\mathfrak{a}$ is reduced and $\mathfrak{a}^*$ is not reduced. We use Theorem 5.5.5.2.

By definition, $\mathfrak{a} = I(\xi)$ and $\mathfrak{a}^* = I(\xi^*)$, where

$$\xi = \frac{\sqrt{D}}{d} \quad \text{and} \quad \xi^* = \frac{\sqrt{D}}{d^*} = \frac{\varepsilon}{\xi} = \begin{pmatrix} 0 & \varepsilon \\ 1 & 0 \end{pmatrix} \xi\,.$$

CASE 1: $\Delta < 0$. Since $\Re(\xi) = \Re(\xi^*) = 0$ and $|\xi^*| < 1 < |\xi|$, it follows that $\mathfrak{a}$ is reduced and $\mathfrak{a}^*$ is not reduced.

CASE 2: $\Delta > 0$. Since

$$\xi + \lfloor -\xi' \rfloor = \frac{\sqrt{D}}{d} + \Bigl\lfloor \frac{\sqrt{D}}{d} \Bigr\rfloor > 1 \quad \text{and} \quad \xi^* + \lfloor -\xi^{*\prime} \rfloor = \frac{\sqrt{D}}{d^*} + \Bigl\lfloor \frac{\sqrt{D}}{d^*} \Bigr\rfloor < 1\,,$$

it follows again that $\mathfrak{a}$ is reduced and $\mathfrak{a}^*$ is not reduced.

2. As $\mathcal{O}_\Delta$ contains ambiguous ideals of type (II), Theorem 5.6.4 implies that $\Delta \equiv 1 \bmod 4$ or $\Delta \equiv 12 \bmod 16$ or $\Delta \equiv 0 \bmod 32$. We prove first that $d \ne d^*$ (and thus $\mathfrak{a} \ne \mathfrak{a}^*$). Indeed, if $d = d^*$, then $\Delta = \varepsilon d^2$, hence $\varepsilon = -1$, $4c = d(1-\varepsilon) = 2d$, and as $(c,d) = (c,2c) = 1$, we get $c = 1$ and $\Delta = -4$, a contradiction.

Since $d^2 - \Delta = d(d - \varepsilon d^*) = 4cd$ and $(c, d^*) = (c,d) = 1$, it follows that $\mathfrak{a}$ and $\mathfrak{a}^*$ are $\mathcal{O}_\Delta$-regular ideals of type (II). Conversely, if $\mathfrak{a}$ is an $\mathcal{O}_\Delta$-regular ideal of type (II), then

$$\mathfrak{a} = \Big[a, \frac{a+\sqrt{\Delta}}{2}\Big], \quad \text{where} \quad a \in \mathbb{N}, \quad 4a \,|\, a^2 - \Delta \quad \text{and} \quad \Big(a, \frac{a^2-\Delta}{4a}\Big) = 1\,.$$

In particular, $a \,|\, \Delta$, and if $d = a$ and $\Delta = \varepsilon dd^*$, where $\varepsilon \in \{\pm 1\}$ and $d^* \in \mathbb{N}$, then

$$d - \varepsilon d^* = \frac{a^2 - \Delta}{a} = 4c\,, \quad \text{where } c \in \mathbb{Z} \text{ and } (c,d) = 1\,.$$

Thus we have proved that $\mathfrak{a}$ and $\mathfrak{a}^*$ are distinct $\mathcal{O}_\Delta$-regular ambiguous ideals of type (II), and all $\mathcal{O}_\Delta$-regular ambiguous ideals of type (II) in $\mathcal{O}_\Delta$ arise in this way. Since

$$\mathfrak{a}\sqrt{\Delta} = \Big[d\sqrt{\Delta}\,, \frac{\Delta + d\sqrt{\Delta}}{2}\Big] = \Big[\Delta, \frac{\Delta + d\sqrt{\Delta}}{2}\Big] = d\,\Big[\varepsilon d^*, \frac{\varepsilon d^* + \sqrt{\Delta}}{2}\Big] = d\mathfrak{a}^*\,,$$

we obtain $\mathfrak{a}^* = d^{-1}\sqrt{\Delta}\,\mathfrak{a} \sim \mathfrak{a}$. If $\Delta > 0$, then Theorem 5.5.4.3 implies that $\mathfrak{a} \sim_+ \mathfrak{a}^*$ if and only if $\mathcal{N}(\varepsilon_\Delta) = -1$. It remains to prove the assertion concerning reduced ideals. We use Theorem 5.5.5.2.

By definition, $\mathfrak{a} = I(\xi)$ and $\mathfrak{a}^* = I(\xi^*)$, where

$$\xi = \frac{1}{2} + \frac{\sqrt{\Delta}}{2d}\,, \quad \xi^* = \frac{1}{2} + \frac{\sqrt{\Delta}}{2d^*}\,, \quad \text{and} \quad \xi^* = A\xi \;\text{ with }\; A = \begin{pmatrix} 1 & \frac{\varepsilon - 1}{2} \\ 2 & -1 \end{pmatrix}.$$

CASE 1: $\Delta > 0$. Since

$$\xi + \lfloor -\xi' \rfloor = \frac{1}{2} + \frac{\sqrt{\Delta}}{2d} + \Big\lfloor -\frac{1}{2} + \frac{\sqrt{\Delta}}{2d} \Big\rfloor > 1 \quad \text{and} \quad \xi^* + \lfloor -\xi^{*\prime} \rfloor < 1\,,$$

it follows that $\mathfrak{a}$ is reduced and $\mathfrak{a}^*$ is not reduced.

CASE 2: $\Delta < 0$. Since

$$\xi = \frac{1}{2} + \mathsf{i}\frac{\sqrt{|\Delta|}}{2d} \quad \text{and} \quad \xi^* = \frac{1}{2} + \mathsf{i}\frac{\sqrt{|\Delta|}}{2d^*}\,,$$

it follows that $\mathfrak{a}$ is reduced if and only if $\xi \in \mathcal{F}$, and $\mathfrak{a}^*$ is reduced if and only if $\xi^* \in \mathcal{F}$. Hence $\mathfrak{a}$ is reduced if and only if

$$\frac{\sqrt{|\Delta|}}{2d} \geq \frac{\sqrt{3}}{2}\,, \quad \text{which is equivalent to} \quad d^* \geq 3d\,.$$

By the same reason, $\mathfrak{a}^*$ is reduced if and only if $d \geq 3d^*$, but since $d < d^* < 3d^*$, it follows that $\mathfrak{a}^*$ is never reduced. If

$$\widetilde{\xi} = \frac{2c - d + \sqrt{\Delta}}{2c} = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \xi\,, \quad \text{then} \quad I(\widetilde{\xi}) = \Big[c, \frac{2c - d + \sqrt{\Delta}}{2}\Big] = \widetilde{\mathfrak{a}}\,.$$

Hence $\widetilde{\mathfrak{a}}$ is an $\mathcal{O}_\Delta$-regular ideal which is equivalent to $\mathfrak{a}$ by Theorem 5.5.7.1. Since

$$|\,\widetilde{\xi}\,|^2 = \frac{(2c-d)^2 - \Delta}{4c^2} = 1 \quad \text{and} \quad \Re(\,\widetilde{\xi}\,) = 1 - \frac{d}{2c}\,,$$

it follows by Theorem 5.5.5.3 that $\widetilde{\mathfrak{a}}$ is reduced if and only if $\widetilde{\xi} \in \mathcal{F}$, that is, if and only if $\Re(\widetilde{\xi}) \in \big[0, \frac{1}{2}\big]$, and this is equivalent $d^* \leq 3d$.

It remains to prove that $d^* \neq 3d$. Once this is done, it follows that $\mathfrak{a}$ is reduced if $d^* > 3d$, and $\widetilde{\mathfrak{a}}$ is reduced if $d^* < 3d$. Assume to the contrary that $d^* = 3d$. Then $c = d + d^* = 4d$, $1 = (c,d) = d$, and $\Delta = -3d^2 = -3$, a contradiction.

We assert that $\mathfrak{a}$ is uniquely determined by $\widetilde{\mathfrak{a}}$. Thus suppose that $\mathfrak{a}$ and $\mathfrak{a}_1$ are ideals such that $\widetilde{\mathfrak{a}} = \widetilde{\mathfrak{a}_1}$. To be precise, assume that $\Delta = -dd^* = -d_1d_1^*$, where $d,\, d^*,\, d_1,\, d_1^* \in \mathbb{N}$, $d < d^*$, $d_1 < d_1^*$, $d + d^* = 4c$, $d_1 + d_1^* = 4c_1$ for some $c,\, c_1 \in \mathbb{N}$,

$$\mathfrak{a} = \Big[d, \frac{d+\sqrt{\Delta}}{2}\Big], \quad \mathfrak{a}_1 = \Big[d_1, \frac{d_1+\sqrt{\Delta}}{2}\Big], \quad \text{and} \quad \widetilde{\mathfrak{a}} = \widetilde{\mathfrak{a}_1}\,,$$

that is,

$$\Big[c, \frac{-d+\sqrt{\Delta}}{2}\Big] = \Big[c_1, \frac{-d_1+\sqrt{\Delta}}{2}\Big].$$

Then Theorem 5.4.2 implies $c = c_1$ and $d \equiv d_1 \bmod 2c$. However, $d < d^*$ implies $d < 2c$, and $d_1 < d_1^*$ implies $d_1 < 2c$. Hence it follows that $|d - d_1| < 2c$ and therefore $d = d_1$ and $\mathfrak{a} = \mathfrak{a}_1$.

3. In 1., we have proved that every $\mathcal{O}_\Delta$-regular ideal of type (I) occurs in exactly one ambiguous pair, and in 2. we have done the same for $\mathcal{O}_\Delta$-regular ideals of type (II). In the course of the proof of 2., we have already seen that $\mathfrak{a}$ is uniquely determined by $\widetilde{\mathfrak{a}}$. □

We continue with some additional preparations. The following definitions and the elementary Lemma 5.6.8 make sense for arbitrary discriminants. Their importance however lies in the case of positive discriminants where they are connected with the corresponding notions in the theory of continued fractions (see Section 2.3). Recall that a quadratic irrational ξ of type (a,b,c) and discriminant Δ is called

- *symmetric* if $c = -a$;
- *ambiguous* if $a \,|\, b$;
- *weakly ambiguous* if $\xi \sim \xi'$.

An $\mathcal{O}_\Delta$-regular ideal $\mathfrak{a}$ is called *symmetric* if $\mathfrak{a} = I(\xi)$ for some reduced symmetric quadratic irrational ξ.

In the following (simple) Lemma we connect the notions for quadratic irrationals with those for ideals.

Lemma 5.6.8. *Let Δ be a quadratic discriminant.*

1. *An $\mathcal{O}_\Delta$-regular ideal $\mathfrak{a}$ is symmetric if and only if*

$$\mathfrak{a} = \Big[\,a, \frac{b+\sqrt{\Delta}}{2}\,\Big], \quad \textit{where} \;\; a,\, b \in \mathbb{N}\,, \;\; (a,b) = 1 \;\; \textit{and} \;\; \Delta = 4a^2 + b^2.$$

   In particular, every symmetric ideal is reduced.

2. *Let ξ be a quadratic irrational of discriminant Δ and $\mathfrak{a} = I(\xi)$.*
   (a) *$\mathfrak{a}$ is ambiguous if and only if ξ is ambiguous.*
   (b) *The ideal class $[\mathfrak{a}] \in \mathcal{C}_\Delta$ is ambiguous if and only if ξ is weakly ambiguous.*
   (c) *If $\mathfrak{a}$ is symmetric, then $[\mathfrak{a}]$ is ambiguous.*

Proof. 1. If $\mathfrak{a}$ is a symmetric $\mathcal{O}_\Delta$-regular ideal, then $\mathfrak{a} = I(\xi)$, where ξ is a quadratic irrational of type $(a, b, -a)$ for some $a,\ b \in \mathbb{N}$. In this case, it follows that $(a, b) = 1,\ \Delta = 4a^2 + b^2$, and ξ is reduced. Hence $\mathfrak{a}$ is a reduced ideal of the asserted form.

Conversely, if

$$\mathfrak{a} = \Big[\, a, \frac{b+\sqrt{\Delta}}{2} \Big]\,, \quad \text{where } \ a,\ b \in \mathbb{N}\,, \quad (a,b) = 1 \ \text{ and } \ \Delta = 4a^2 + b^2\,,$$

then $\mathfrak{a} = I(\xi)$, where ξ is a quadratic irrational of type $(a, b, -a)$. Since ξ is symmetric, it follows that $\mathfrak{a}$ is symmetric.

2. Let ξ be of type (a, b, c).

(a) By definition, $\mathfrak{a}$ is ambiguous if and only if

$$\Big[a, \frac{b+\sqrt{\Delta}}{2} \Big] = \Big[a, \frac{-b+\sqrt{\Delta}}{2} \Big]\,,$$

and this holds if and only if $b \equiv -b \mod 2a$, which is equivalent to $a \,|\, b$.

(b) By definition, $[\mathfrak{a}]$ is ambiguous if and only if $\mathfrak{a} \sim \mathfrak{a}'$. But this holds if and only if $\xi \sim \xi'$, that is, if and only if ξ is weakly ambiguous.

(c) If $\mathfrak{a}$ is symmetric, we may assume that ξ is symmetric. Then ξ is weakly ambiguous by Theorem 2.3.2.3, and thus $[\mathfrak{a}]$ is ambiguous by (b). □

Let now $\Delta > 0$ be a quadratic discriminant. In this case, we can do more, using the results of the Sections 2.2 and 2.3. Let $C \in \mathcal{C}_\Delta$ be a regular ideal class of $\mathcal{O}_\Delta$, and let $\mathfrak{a} = I(\xi_0) \in C$ be a reduced ideal, where ξ_0 is a reduced quadratic irrational. Let $\mathsf{z} = (\xi_0, \xi_1, \ldots, \xi_{l-1})$ be the period of ξ. Then $\{I(\xi_0), I(\xi_1), \ldots, I(\xi_{l-1})\}$ is the set of all reduced ideals in C. We call $(I(\xi_0), I(\xi_1), \ldots, I(\xi_{l-1}))$ the *cycle* of $\mathfrak{a} = I(\xi_0)$, and $l = l(\mathfrak{a}) = l(C)$ the *period length* of $\mathfrak{a}$ (respectively of C). Note that $\mathcal{N}(\varepsilon_\Delta) = (-1)^l$.

Let now $C \in \mathcal{C}_\Delta$ be an ambiguous class of $\mathcal{O}_\Delta$, $\ \mathfrak{a} \in C$ a reduced ideal, $(\mathfrak{a}_1, \ldots, \mathfrak{a}_l)$ the cycle of $\mathfrak{a}$, and set $\mathfrak{a}_{l+1} = \mathfrak{a}_1$. Since $C = [\mathfrak{a}] = [\mathfrak{a}']$ and $\mathfrak{a}'$ is reduced, there exists a unique index $p = \mathsf{p}(\mathfrak{a}) \in [1, l]$ such that $\mathfrak{a}' = \mathfrak{a}_{p+1}$. Following R. Mollin (see [**73**] and [**74**, Ch. 6]), we call $\mathsf{p}(\mathfrak{a})$ the *palindromic index* of $\mathfrak{a}$.

In the following Theorem 5.6.9 we connect the palindromic index $\mathsf{p}(\xi_0)$ of a reduced weakly ambiguous quadratic irrational ξ_0 (as introduced in Theorem 2.3.4) with the palindromic index of the ideal $I(\xi_0)$, and we rephrase and refine Theorem 2.3.4 in terms of ideals.

Theorem 5.6.9. *Let $\Delta > 0$ be a quadratic discriminant, $C \in \mathcal{C}_\Delta$ an ambiguous class, $\mathfrak{a} \in C$ a reduced ideal, $l = l(\mathfrak{a})$ and $p = \mathsf{p}(\mathfrak{a})$.*

1. *If $\mathfrak{a} = I(\xi_0)$, where ξ_0 is a weakly ambiguous reduced quadratic irrational, then $p = \mathsf{p}(\xi_0) - 1$.*
2. *Let $(\mathfrak{a}_1, \ldots, \mathfrak{a}_l)$ be the cycle of $\mathfrak{a} = \mathfrak{a}_1$, and set $\mathfrak{a}_{j+sl} = \mathfrak{a}_j$ for all $j \in [1, l]$ and $s \in \mathbb{Z}$. Then $\{\mathfrak{a}_1, \ldots, \mathfrak{a}_l\}$ is the set of all reduced ideals in C, and the symmetric and reduced ambiguous ideals in the cycle are given by the following table:*

$l,\ p$	ambiguous ideals	symmetric ideals
$l=2k,\ \ p=2m$	$\mathfrak{a}_{m+1},\ \ \mathfrak{a}_{m+k+1}$	–
$l=2k,\ \ p=2m-1$	–	$\mathfrak{a}_{m+1},\ \ \mathfrak{a}_{m+k+1}$
$l=2k-1,\ \ p=2m$	$\mathfrak{a}_{m+1}$	$\mathfrak{a}_{m+k+1}$
$l=2k-1,\ \ p=2m-1$	$\mathfrak{a}_{m+k}$	$\mathfrak{a}_{m+1}$

In particular:

- *If $\mathcal{N}(\varepsilon_\Delta)=-1$, then C contains exactly one symmetric ideal and exactly one reduced ambiguous ideal.*
- *If $\mathcal{N}(\varepsilon_\Delta)=1$ and p is odd, then C contains exactly two symmetric ideals and no reduced ambiguous ideal.*
- *If $\mathcal{N}(\varepsilon_\Delta)=1$ and p is even, then C contains exactly two reduced ambiguous ideals and no symmetric ideal.*

PROOF. Suppose that $\mathfrak{a}=I(\xi_0)$, where ξ_0 is a weakly ambiguous reduced quadratic irrational. Let $(\xi_0,\ldots,\xi_{l-1})$ be the period of ξ_0 and $(\xi_i)_{i\in\mathbb{Z}}$ its periodic extension. For $i\in\mathbb{Z}$, we set $\mathfrak{a}_i=I(\xi_{i-1})$. Then $(\mathfrak{a}_1,\ldots,\mathfrak{a}_l)$ is the cycle of $\mathfrak{a}$. If $n=\mathsf{p}(\xi_0)$, then the Theorems 2.3.4 and 1.3.5.3(b) imply $\xi_n=-\xi_0'^{-1}=(-\xi_0'+\lfloor\xi_0\rfloor)^{\#}$, hence $\xi_{n-1}=-\xi_0'+\lfloor\xi_0\rfloor$, and $\mathfrak{a}_n=I(\xi_{n-1})=I(\xi_0')=\mathfrak{a}'$. Thus we obtain $p=n-1$, and the assertions follow immediately by Theorem 2.3.4. □

Exercise 5.6.10. Let $\Delta=45305=5\cdot13\cdot17\cdot41$. Prove that $h_\Delta=8$ and all classes $C\in\mathcal{C}_\Delta$ are ambiguous. Determine all ambiguous and symmetric ideals and their distribution in the various classes. (Compare [**74**, Example 6.1.3].)

In order to obtain a well-arranged formulation of the subsequent main theorem on ambiguous classes, we introduce the following notations.

Let Δ be a quadratic discriminant. We denote by

- $\mathcal{A}_\Delta^{(+)}$ the set of all regular ideal classes of $\mathcal{O}_\Delta$;
- $\mathcal{A}_\Delta^*$ the set of all ideal classes of $\mathcal{O}_\Delta$ which contain an ambiguous ideal;
- $\mu(\Delta)$ the *Gauss number*, defined by

$$\mu(\Delta)=\begin{cases} r & \text{if} \quad \Delta\equiv 1 \bmod 4 \quad \text{or} \quad \Delta\equiv 4 \bmod 16\,,\\ r+1 & \text{if} \quad \Delta\equiv 8 \text{ or } 12 \bmod 16 \quad \text{or} \quad \Delta\equiv 16 \bmod 32\,,\\ r+2 & \text{if} \quad \Delta\equiv \quad \bmod 32\,.\end{cases}$$

By Theorem 5.6.4.B, $2^{\mu(\Delta)}$ is the number of $\mathcal{O}_\Delta$-regular ambiguous ideals. By Theorem 5.6.1 and Corollary A.5.5, it follows that

$$\mathcal{A}_\Delta^{(+)}=\mathcal{C}_\Delta^{(+)}[2]=\{C\in\mathcal{C}_\Delta^{(+)}\mid C^2=[\mathcal{O}_\Delta^{(+)}]\,\}\quad\text{and}\quad |\mathcal{A}_\Delta^{(+)}|=2^{\mathsf{r}_2(\mathcal{C}_\Delta^{(+)})}=|\mathcal{C}_\Delta^{(+)}/\mathcal{C}_\Delta^{(+)\,2}|\,.$$

By the very definition, $\mathcal{A}_\Delta^*$ is a subgroup of $\mathcal{A}_\Delta$. By the Theorems 5.5.4.2 and 5.6.2 it follows that

$$\mathcal{A}_\Delta=\mathcal{A}_\Delta^+=\mathcal{A}_\Delta^*\quad\text{unless}\quad\Delta>0\ \text{ and }\ \mathcal{N}(\varepsilon_\Delta)=1\,.$$

Moreover, the product of two classes in $\mathcal{A}_\Delta \setminus \mathcal{A}^*_\Delta$ belongs to $\mathcal{A}^*_\Delta$, and therefore

$$(\mathcal{A}_\Delta : \mathcal{A}^*_\Delta) \le 2\,.$$

We say that an ambiguous class $C \in \mathcal{A}_\Delta$ contains an ambiguous pair $(\mathfrak{a}, \mathfrak{a}^*)$ of $\mathcal{O}_\Delta$ if $\{\mathfrak{a}, \mathfrak{a}^*\} \subset C$.

Theorem 5.6.11 (Main theorem on ambiguous classes)**.** *Let Δ be a quadratic discriminant.*

1. *Suppose that either $\Delta < 0$, or $\Delta > 0$ and $\mathcal{N}(\varepsilon_\Delta) = -1$. Then every ambiguous class $C \in \mathcal{A}_\Delta$ contains exactly one ambiguous pair, and*

$$|\mathcal{A}_\Delta| = 2^{\mu(\Delta)-1}\,.$$

2. *Suppose that $\Delta > 0$ and $\mathcal{N}(\varepsilon_\Delta) = 1$. Then every ambiguous class $C \in \mathcal{A}_\Delta$ contains exactly two ambiguous pairs,*

$$\mu(\Delta) \ge 2\,, \quad |\mathcal{A}^*_\Delta| = 2^{\mu(\Delta)-2}\,, \quad |\mathcal{A}^+_\Delta| = 2^{\mu(\Delta)-1},$$

and

$$|\mathcal{A}_\Delta| = \begin{cases} 2^{\mu(\Delta)-1} & \textit{if} \quad \Delta = 4a^2 + b^2\,, \quad \textit{where } a, b \in \mathbb{N} \textit{ and } (a,b) = 1\,, \\ 2^{\mu(\Delta)-2} & \textit{otherwise.} \end{cases}$$

PROOF. 1. By Theorem 5.6.7.3, there exist exactly $2^{\mu(\Delta)-1}$ ambiguous pairs of $\mathcal{O}_\Delta$, and thus it suffices to prove that every class $C \in \mathcal{A}_\Delta$ contains exactly one ambiguous pair.

Let $C \in \mathcal{A}_\Delta$ be an ambiguous class. If $(\mathfrak{a}, \mathfrak{a}^*)$ is an ambiguous pair, then $\mathfrak{a} \sim \mathfrak{a}^*$ and since C contains an $\mathcal{O}_\Delta$-regular ambiguous ideal, it contains some ambiguous pair. We must prove that this is the only one. Thus let $(\mathfrak{a}_1, \mathfrak{a}_1^*)$ be any ambiguous pair in C.

If $\Delta > 0$, then $\mathfrak{a}$ and $\mathfrak{a}_1$ are both reduced ambiguous ideals, but, by Theorem 5.6.9.2, C contains only one reduced ambiguous ideal, and thus $\mathfrak{a} = \mathfrak{a}_1$.

If $\Delta < 0$, then (by Theorem 5.6.7) there exist reduced ideals $\widetilde{\mathfrak{a}}$ and $\widetilde{\mathfrak{a}}_1$ such that $\mathfrak{a} \sim \widetilde{\mathfrak{a}}$ and $\mathfrak{a}_1 \sim \widetilde{\mathfrak{a}}_1$. Hence $\{\widetilde{\mathfrak{a}}, \widetilde{\mathfrak{a}}_1\} \subset C$, and therefore $\widetilde{\mathfrak{a}} = \widetilde{\mathfrak{a}}_1$ by Theorem 5.5.7.2(a). By Theorem 5.6.7.3, $\widetilde{\mathfrak{a}} = \widetilde{\mathfrak{a}}_1$ implies $\mathfrak{a} = \mathfrak{a}_1$.

2. By Theorem 5.6.9.2, every class $C \in \mathcal{A}^*_\Delta$ contains exactly two reduced ambiguous ideals, and since in each ambiguous pair there is exactly one reduced ideal, it follows that C contains exactly two ambiguous pairs. Hence we get $\mu(\Delta) \ge 2$, and $|\mathcal{A}^*_\Delta| = 2^{\mu(\Delta)-2}$. By Theorem 5.5.4.3, every class $C \in \mathcal{A}_\Delta$ splits into two narrow classes, and by Theorem 5.6.2.1, every narrow ambiguous class contains an ambiguous ideal. Therefore we obtain $|\mathcal{A}^+_\Delta| = 2|\mathcal{A}^*_\Delta| = 2^{\mu(\Delta)-1}$.

If $\Delta = 4a^2 + b^2$, where $a, b \in \mathbb{N}$ and $(a,b) = 1$, then $\mathcal{O}_\Delta$ contains a symmetric ideal $\mathfrak{a}$ by Lemma 5.6.8, and by Theorem 5.6.9 $[\mathfrak{a}]$ is an ambiguous class without ambiguous ideals. This implies $\mathcal{A}^*_\Delta \ne \mathcal{A}_\Delta$, and therefore $|\mathcal{A}_\Delta| = 2\,|\mathcal{A}^*_\Delta| = 2^{\mu(\Delta)-1}$.

If Δ is not of the form $\Delta = 4a^2 + b^2$, where $a, b \in \mathbb{N}$ and $(a,b) = 1$, then there are no symmetric ideals in $\mathcal{O}_\Delta$, and therefore $\mathcal{A}_\Delta = \mathcal{A}^*_\Delta$. □

Exercise 5.6.12. Let $\Delta > 0$ be a quadratic discriminant. Prove that the number $\mathsf{s}(\Delta)$ of symmetric ideals in $\mathcal{O}_\Delta$ is given by

$$\mathsf{s}(\Delta) = \begin{cases} 2^{\mu(\Delta)-1} & \text{if} \quad \Delta = 4a^2 + b^2\,, \quad \text{where } a,\, b \in \mathbb{N} \text{ and } (a,b) = 1\,, \\ 0 & \text{otherwise.} \end{cases}$$

Moreover,

- If $\mathcal{N}(\varepsilon_\Delta) = -1$, then $\mathsf{s}(\Delta) > 0$.
- If Δ is a fundamental discriminant and $-1 = \mathcal{N}(\gamma)$ for some $\gamma \in \mathbb{Q}(\sqrt{\Delta}\,)$, then $\mathsf{s}(\Delta) > 0$.

As a simple consequence of Theorem 5.6.11, we list all quadratic discriminants with odd (narrow) class number.

Theorem 5.6.13. *Let Δ be a quadratic discriminant.*

1. *If $\Delta < 0$, then h_Δ is odd if and only if*
   - *either $\Delta \in \{-p^r,\, -4p^r\}$ for some prime $p \equiv 3 \bmod 4$ and odd $r \in \mathbb{N}$,*
   - *or $\Delta \in \{-4,\, -8,\, -16\}$.*
2. *If $\Delta > 0$, then h_Δ^+ is odd if and only if*
   - *either $\Delta \in \{p^r,\, 4p^r\}$ for some prime $p \equiv 1 \bmod 4$ and odd $r \in \mathbb{N}$,*
   - *or $\Delta = 8$.*

   In all these cases we have $\mathcal{N}(\varepsilon_\Delta) = -1$.
3. *If $\Delta > 0$, then h_Δ is odd if and only if*
   - *either h_Δ^+ is odd,*
   - *or $\Delta \in \{p^rq^s,\, 4p^rq^s\}$, where $p \neq q$ are odd primes, r and s are not both even, $p \equiv 3 \bmod 4$ and $p^rq^s \equiv 1 \bmod 4$,*
   - *or $\Delta = 4p^r \equiv 12 \bmod 16$ for some prime p and odd $r \in \mathbb{N}$,*
   - *or $\Delta \in \{8p^r,\, 16p^r\}$ for some prime $p \equiv 3 \bmod 4$ and $r \in \mathbb{N}$,*
   - *or $\Delta = 32$.*
4. *If Δ is a fundamental discriminant, then h_Δ is odd if and only if*
   - *either $\Delta = (-1)^{(p-1)/2}p$ for some odd prime p,*
   - *or $\Delta \in \{4p,\, 8p\}$ for some prime $p \equiv 3 \bmod 4$,*
   - *or $\Delta = pq$ for some primes p, q such that $p \neq q$ and $p \equiv q \equiv 3 \bmod 4$,*
   - *or $\Delta \in \{-4,\, \pm 8\}$.*

Exercise 5.6.14. Provide a detailed proof of Theorem 5.6.13.

5.7. An application: Some binary Diophantine equations

We apply the structure theory of regular ambiguous ideals and ambiguous ideal classes for the investigation of certain binary quadratic Diophantine equations. There is an extensive literature concerning binary Diophantine equations. Among others, we refer to the following papers for more details: [**88**], [**76**], [**36**], [**79**], [**29**], [**56**], [**77**], [**49**] [**103**], [**26**], [**39**]. In these papers an interested reader my find further applications of continued fractions and ideal theory to Diophantine equations, stronger results for special cases and proofs using other methods.

Theorem 5.7.1. *Let* $p \equiv 1 \bmod 4$ *be a prime and* r *an odd positive integer.*

1. *If* $\Delta \in \{8, p^r, 4p^r\}$, *then* $\mathcal{N}(\varepsilon_\Delta) = -1$, $\mathcal{O}_\Delta$ *contains exactly one symmetric ideal, and this is a principal ideal generated by a norm-positive element.*
2. *Suppose that* $p^r = 4a^2 + b^2$, *where* $a,\, b \in \mathbb{N}$ *and* $(a, b) = 1$.
   (a) *There exist* $x,\, y \in \mathbb{Z}$ *such that* $(x, y) \,|\, 2$ *and* $x^2 - p^r y^2 = 4a$.
   (b) *There exist* $x,\, y \in \mathbb{Z}$ *such that* $(x, y) = 1$ *and* $x^2 - p^r y^2 = b$.

Proof. Suppose that $\Delta \in \{8, p^r, 4p^r\}$. Then $\mu(\Delta) = 1$, by Theorem 5.6.11 it follows that $\mathcal{N}(\varepsilon_\Delta) = -1$, $|\mathcal{A}_\Delta| = 1$, and $\mathcal{O}_\Delta$ contains exactly one symmetric ideal $\mathfrak{a}$. It is principal since the principal class is the only ambiguous class of $\mathcal{O}_\Delta$, and since $\mathcal{N}(\varepsilon_\Delta) = -1$, we may assume that $\mathfrak{a} = \alpha\mathcal{O}_\Delta$ for some $\alpha \in \mathcal{O}_\Delta^\bullet$ such that $\mathfrak{N}_\Delta(\mathfrak{a}) = \mathcal{N}(\alpha) > 0$. Hence 1. holds, and for the proof of 2. we apply Lemma 5.6.8.1.

(a) If $\Delta = p^r$, then

$$\mathfrak{a} = \Big[\, a,\, \frac{b + \sqrt{p^r}}{2} \,\Big] = \alpha\mathcal{O}_\Delta\,, \quad \text{where} \quad \alpha \in \mathcal{O}_\Delta^\bullet \quad \text{is primitive}\,,$$

and we set

$$\alpha = \frac{x + y\sqrt{p^r}}{2} \in \mathcal{O}_\Delta^\bullet\,, \quad \text{where} \;\; x,\, y \in \mathbb{Z}\,, \;\; x \equiv y \bmod 2, \;\; (x, y) \,|\, 2 \;\; \text{and} \;\; \mathcal{N}(\alpha) = a\,.$$

Then it follows that $4a = x^2 - p^r y^2$.

(b) If $\Delta = 4p^r = 4b^2 + 4(2a)^2$, then, observing that $(b, 2a) = 1$, we obtain

$$\mathfrak{a} = [b, a + \sqrt{p^r}\,] = \alpha\mathcal{O}_\Delta\,, \quad \text{where} \quad \alpha = x + y\sqrt{p^r} \in \mathcal{O}_\Delta^\bullet \quad \text{is primitive}\,,$$

$x,\, y \in \mathbb{Z}$, $(x, y) = 1$, and $\mathcal{N}(\alpha) = x^2 - p^r y^2 = b$. □

Theorem 5.7.2. *Let* $\Delta > 0$ *be a quadratic discriminant.*

1. *Suppose that* $\Delta = 4D \equiv 0 \bmod 4$,
   - $c \in \{1, 2\}$ *if* $8 \,|\, D$, *and* $c = 1$ *if* $8 \nmid D$;
   - $t \in \{1, 2\}$ *if* $D \equiv 3 \bmod 4$, *and* $t = 1$ *if* $D \not\equiv 3 \bmod 4$;
   - $D = c^2 d d^*$, *where* $d,\, d^* \in \mathbb{N}$ *and* $(d, d^*) = 1$,

and set

$$\mathfrak{j} = \begin{cases} [d, \sqrt{D}\,] & \text{if} \quad ct = 1\,, \\ [2d, d+\sqrt{D}\,] & \text{if} \quad t = 2\,, \\ [4d, 2d+\sqrt{D}\,] & \text{if} \quad c = 2\,. \end{cases}$$

(a) $\mathfrak{j}$ *is an* $\mathcal{O}_\Delta$*-regular ambiguous ideal satisfying* $\mathfrak{N}_\Delta(\mathfrak{j}) = c^2dt$*, and every* $\mathcal{O}_\Delta$*-regular ambiguous ideal is of this form.*

$\mathfrak{j}$ *is reduced if and only if* $d < d^*$*, and* $\mathfrak{j}$ *is a principal ideal if and only if there exist* $x,\ y \in \mathbb{Z}$ *such that* $|dx^2 - d^*y^2| = t$ *and* $(c, xy) = 1$*.*

(b) *Let* $x,\ y \in \mathbb{Z}$ *be such that* $|dx^2 - d^*y^2| = t$ *and* $(c, xy) = 1$*. Then*

$$\mathfrak{j} = (cdx + y\sqrt{D}\,)\,\mathcal{O}_\Delta\,.$$

2. *Suppose that* $\Delta \equiv 1 \bmod 4$ *and* $\Delta = dd^*$*, where* $d,\ d^* \in \mathbb{N}$*,* $(d, d^*) = 1$*, and set*

$$\mathfrak{j} = \Big[\, d, \frac{d+\sqrt{\Delta}}{2}\,\Big]\,.$$

(a) $\mathfrak{j}$ *is an* $\mathcal{O}_\Delta$*-regular ambiguous ideal satisfying* $\mathfrak{N}_\Delta(\mathfrak{j}) = d$*, and every* $\mathcal{O}_\Delta$*-regular ambiguous ideal is of this form.*

$\mathfrak{j}$ *is reduced if and only if* $d < d^*$*, and* $\mathfrak{j}$ *is a principal ideal if and only if there exist* $x,\ y \in \mathbb{Z}$ *such that* $|dx^2 - d^*y^2| = 4$*.*

(b) *Let* $x,\ y \in \mathbb{Z}$ *be such that* $|dx^2 - d^*y^2| = 4$*. Then*

$$\mathfrak{j} = \frac{dx + y\sqrt{\Delta}}{2}\,\mathcal{O}_\Delta\,.$$

PROOF. 1.(a) By Theorem 5.6.4, $\mathfrak{j}$ is an $\mathcal{O}_\Delta$-regular ambiguous ideal satisfying $\mathfrak{N}_\Delta(\mathfrak{j}) = c^2dt$, every $\mathcal{O}_\Delta$-regular ambiguous ideal is of this form, and we apply Theorem 5.6.7. In any case, $\mathfrak{j}$ is reduced if and only if $d < d^*$.

Let now $\mathfrak{j}$ be principal, say $\mathfrak{j} = (u + y\sqrt{D}\,)\,\mathcal{O}_\Delta$, where $u,\ y \in \mathbb{Z}$ and $(u, y) = 1$.

If $ct = 1$, then $D = dd^*$, and $u + y\sqrt{D} \in \mathbb{Z}d + \mathbb{Z}\sqrt{D}$ implies that $u = dx$ for some $x \in \mathbb{Z}$. Since $d = \mathfrak{N}_\Delta(\mathfrak{j}) = |\mathcal{N}(dx + y\sqrt{D}\,)| = |d^2x^2 - dd^*y^2|$, it follows that $|dx^2 - d^*y^2| = 1$.

If $t = 2$, then $u + y\sqrt{D} \in \mathbb{Z}(2d) + \mathbb{Z}(d + \sqrt{D}\,)$ implies $u + y\sqrt{D} = 2dv + (d + \sqrt{D}\,)w$ for some $v,\ w \in \mathbb{Z}$, and if $x = 2v + w$, then $u = dx$ and $y = w$. Since $D = dd^*$, it follows that $2d = \mathfrak{N}_\Delta(\mathfrak{j}) = |\mathcal{N}(dx + y\sqrt{D}\,)| = |d^2x^2 - dd^*y^2|$, and therefore $|dx^2 - d^*y^2| = 2$.

If $c = 2$, then $u + y\sqrt{D} \in \mathbb{Z}(4d) + \mathbb{Z}(2d + \sqrt{D}\,)$, and there exist $v,\ w \in \mathbb{Z}$ such that $u + y\sqrt{D} = 4dv + (2d + \sqrt{D}\,)w$. If $x = 2v + w$, then $u = 2dx$, $y = w$, and $2 \nmid xy$. It follows that $4d = \mathfrak{N}_\Delta(\mathfrak{j}) = |\mathcal{N}(2dx + y\sqrt{D}\,)| = |4d^2x^2 - 4dd^*y^2|$, and therefore $|dx^2 - d^*y^2| = 1$.

The converse holds by (b).

(b) If $ct = 1$, then $dx + y\sqrt{D} \in \mathfrak{j}$, hence $(dx + y\sqrt{D}\,)\mathcal{O}_\Delta \subset \mathfrak{j}$, and equality holds, since $\mathfrak{N}_\Delta\big((dx + y\sqrt{D}\,)\mathcal{O}_\Delta\big) = |\mathcal{N}(dx + y\sqrt{D}\,)| = |d^2x^2 - dd^*y^2| = d = \mathfrak{N}_\Delta(\mathfrak{j})$.

If $t=2$, then $D=dd^*\equiv 3 \bmod 4$, hence $2\nmid xy$, and $x-y=2u$ for some $u\in\mathbb{Z}$. We get $dx+y\sqrt{D}=2du+(d+\sqrt{D}\,)y\in\mathfrak{j}$, hence $(dx+y\sqrt{D}\,)\,\mathcal{O}_\Delta\subset\mathfrak{j}$, and equality holds, since $\mathfrak{N}_\Delta\big((dx+y\sqrt{D}\,)\mathcal{O}_\Delta\big)=|\mathcal{N}(dx+y\sqrt{D}\,)|=|d^2x^2-dd^*y^2|=2d=\mathfrak{N}_\Delta(\mathfrak{j})$.

If $c=2$ and $2\nmid xy$, then $D=4dd^*$ and $x-y=2u$ for some $u\in\mathbb{Z}$, which implies $2dx+y\sqrt{D}=4du+(2d+\sqrt{D}\,)y\in\mathfrak{j}$. Hence $(dx+y\sqrt{D}\,)\,\mathcal{O}_\Delta\subset\mathfrak{j}$, and equality holds, since $\mathfrak{N}_\Delta\big((2dx+y\sqrt{D}\,)\mathcal{O}_\Delta\big)=|\mathcal{N}(2dx+y\sqrt{D}\,)|=|4d^2x^2-4dd^*y^2|=4d=\mathfrak{N}_{4D}(\mathfrak{j})$.

The proof of 2. is done in the same way and is left as an exercise. $\square$

Exercise 5.7.3. Prove Theorem 5.7.2.2.

The following remark addresses the Diophantine equation $|dx^2-d^*y^2|=1$ if $c=2$ and $2\,|\,xy$.

Remark 5.7.4. Let $D\in\mathbb{N}$ be not a square, $8\,|\,D$ and $D=4dd^*$, where $d,\ d^*\in\mathbb{N}$ and $(d,d^*)=1$. Let $x,\ y\in\mathbb{Z}$ be such that $|dx^2-d^*y^2|=1$.

1. If $2\,|\,x$, then $(2dx+y\sqrt{D}\,)\mathcal{O}_{4D}=[4d,\sqrt{D}\,]$. Indeed, if $x=2x_1$, where $x_1\in\mathbb{Z}$, then $|4dx_1^2-d^*y^2|=1$ and $D=(4d)d^*$. Hence the assertion follows by Theorem 5.7.2.2(a).
2. If $2\,|\,y$ and $y=2y_1$, then $(dx+y_1\sqrt{D}\,)\mathcal{O}_{4D}=[d,\sqrt{D}\,]$. Indeed, in this case $|dx^2-4d^*y_1^2|=1$ and $D=d(4d^*)$. Hence again the assertion follows by Theorem 5.7.2.2(a).

Theorem 5.7.5. *Let $D\in\mathbb{N}$ be not a square and $l=l(\sqrt{D}\,)$ the period length of $\sqrt{D}$. Let $\mathcal{L}(D)$ be the set of all quadruples (d,d^*,t,σ) with the following properties:*

- *$d,\ d^*\in\mathbb{N}$ and $(d,d^*)=1$;*
- *$D=c^2dd^*$, where $c\in\{1,2\}$ if $8\,|\,D$, and $c=1$ if $8\nmid D$;*
- *$t\in\{1,2\}$ if $D\equiv 3 \bmod 4$, and $t=1$ if $D\not\equiv 3 \bmod 4$;*
- *$\sigma\in\{\pm1\}$;*
- *there exist $x,\ y\in\mathbb{Z}$ such that $dx^2-d^*y^2=\sigma t$ and $(c,xy)=1$.*

Then $|\mathcal{L}(D)|=4$, and the structure of $\mathcal{L}(D)$ is as follows.

1. *If l is odd, then $\mathcal{L}(D)=\{(1,D,1,\pm1),\ (D,1,1,\pm1)\,\}$.*
2. *If $l=2k$ is even, then*
$$\mathcal{L}(D)=\{(1,D,1,1),\ (D,1,1,-1),\ (d,d^*,t,\sigma),\ (d^*,d,t,-\sigma)\,\}\,,$$
where $1\le d<d^*$ and $cdt\ne1$.
3. *Let $l=2k$ be even, $(d,d^*,t,\sigma)\in\mathcal{L}(D)$, $1\le d<d^*$ and $cdt\ne1$. Let $(p_n)_{n\ge-2}$ be the sequence of partial numerators and $(q_n)_{n\ge-2}$ the sequence of partial denominators of $\sqrt{D}$. Then*
$$\sigma=(-1)^k,\quad p_{k-1}^2-Dq_{k-1}^2=(-1)^kc^2dt\,,\quad c^2dt\,\varepsilon_{4D}=(p_{k-1}+q_{k-1}\sqrt{D}\,)^2,$$
$$c^2dt\,|\,2p_{k-1}\quad\textit{and}\quad \varepsilon_{4D}=(-1)^k+\frac{2d^*}{t}\,q_{k-1}^2+\frac{2p_{k-1}q_{k-1}}{c^2dt}\sqrt{D}\,.$$

PROOF. We shall consistently use Theorem 5.7.2. Note that $(d,d^*,t,\sigma)\in\mathcal{L}(D)$ if and only if $(d^*,d,t,-\sigma)\in\mathcal{L}(D)$.

1. If l is odd, then $\mathcal{N}(\mathcal{O}_{4D}^\times)=\{\pm1\}$ and $\{\,(1,D,1,\pm1),\ (D,1,1,\pm1)\,\}\subset\mathcal{L}(D)$. Theorem 5.2.2 implies $D\not\equiv 3 \mod 4$, hence $t=1$, and, by Theorem 5.6.9, the unit ideal $\mathcal{O}_{4D}=\mathbb{Z}+\mathbb{Z}\sqrt{D}$ is the only reduced ambiguous ideal in the principal class of $\mathcal{O}_{4D}$. Assume that, contrary to our assertion, there exists some $(d,d^*,1,\sigma)\in\mathcal{L}(D)$ such that $1\le d<d^*$ and $cd>1$. Then there exists some reduced ambiguous principal ideal $\mathfrak{j}\subset\mathcal{O}_{4D}$ such that $\mathfrak{N}_{4D}(\mathfrak{j})=c^2d$, a contradiction.

2. Let $l=2k$ be even, hence $\mathcal{N}(\mathcal{O}_{4D}^\times)=\{1\}$. We prove first:

A. If $(d,d^*,t,\sigma)\in\mathcal{L}(D)$, then $(d,d^*,t,-\sigma)\notin\mathcal{L}(D)$.

Proof of **A.** Assume to the contrary that there is some $(d,d^*,t,\sigma)\in\mathcal{L}(D)$ such that $(d,d^*,t,-\sigma)\in\mathcal{L}(D)$. Then there exist integers $x,\ y,\ x_1,\ y_1\in\mathbb{Z}$ such that $dx^2-d^*y^2=\sigma t,\ dx_1^2-d^*y_1^2=-\sigma t$ and $(c,xy)=(c,x_1y_1)=1$. Hence it follows that $(cdx+y\sqrt{D}\,)\,\mathcal{O}_{4D}=(cdx_1+y_1\sqrt{D}\,)\,\mathcal{O}_{4D}$, and thus $cdx_1+y_1\sqrt{D}=\varepsilon(cdx+y\sqrt{D}\,)$ for some $\varepsilon\in\mathcal{O}_{4D}^\times$. Taking norms, we obtain

$$-c^2d\sigma t=\mathcal{N}(cdx_1+y_1\sqrt{D}\,)=\mathcal{N}(\varepsilon)\mathcal{N}(cdx+y\sqrt{D}\,)=\mathcal{N}(\varepsilon)\,c^2d\sigma t\,,$$

and consequently $\mathcal{N}(\varepsilon)=-1$, a contradiction. □[**A.**]

By Theorem 5.6.9, the principal class of $\mathcal{O}_{4D}$ contains precisely one reduced ambiguous ideal $\mathfrak{j}$ distinct from the unit ideal, and this ideal gives rise to an equation $|dx^2-d^*y^2|=t$, where $d,\ d^*\in\mathbb{N}$ and $x,\ y\in\mathbb{Z}$ are such that $1\le d<d^*,\ (d,d^*)=1$, $D=c^2dd^*$, $cdt>1$ and $(c,xy)=1$. Hence there exists some $\sigma\in\{\pm1\}$ such that $(d,d^*,t,\sigma)\in\mathcal{L}(D)$. To prove uniqueness, we must show:

B. If $(d_1,d_1^*,t_1,\sigma_1),\ (d_2,d_2^*,t_2,\sigma_2)\in\mathcal{L}(D),\ \ 1\le d_1<d_1^*,\ \ c_1t_1d_1>1,$ and $1\le d_2<d_2^*,\ c_2t_2d_2>1$, then $(d_1,d_1^*,t_1,\sigma_1)=(d_2,d_2^*,t_2,\sigma_2)$.

Proof of **B.** For $i\in\{1,2\}$, suppose that $(d_i,d_i^*,t_i,\sigma_i)\in\mathcal{L}(D),\ 1\le d_i<d_i^*$ and $c_it_id_i>1$, where $c_i\in\{1,2\}$ are such that $D=c_i^2d_id_i^*$. Then there exist integers $x_i,\ y_i\in\mathbb{Z}$ such that $(c_i,x_iy_i)=1$, and the ideal

$$\mathfrak{j}_i=(c_id_ix_i+y_i\sqrt{D})\,\mathcal{O}_{4D}=\begin{cases}[d_i,\sqrt{D}\,] & \text{if}\quad c_it_i=1\,,\\ [2d_i,d_i+\sqrt{D}\,] & \text{if}\quad t_i=2\,,\\ [4d_i,2d_i+\sqrt{D}\,] & \text{if}\quad c_i=2\end{cases}$$

is a reduced ambiguous ideal distinct from the unit ideal in the principal class of $\mathcal{O}_{4D}$. Hence it follows that $\mathfrak{j}_1=\mathfrak{j}_2$, and in particular $\mathfrak{N}_{4D}(\mathfrak{j}_1)=\mathfrak{N}_{4D}(\mathfrak{j}_2)$, which implies $c_1^2t_1d_1=c_2^2t_2d_2$.

If $t_1=2$, then $D\equiv 3 \mod 4$, hence $c_1=c_2=1$. Since $2d_1=t_2d_2$ and d_2 is odd, it follows that $t_2=2,\ d_1=d_2,\ d_1^*=d_2^*$, and **A** implies $\sigma_1=\sigma_2$. By symmetry, the assertion also holds if $t_1=2$, and thus we may assume that $t_1=t_2=1$.

Suppose that $c_1\ne c_2$, say $c_1=2$ and $c_2=1$. Then we obtain $4d_1=d_2$ and $[4d_1,2d_1+\sqrt{D}\,]=[d_2,\sqrt{D}\,]=[4d_1,\sqrt{D}\,]$, a contradiction. Hence it follows that $c_1=c_2,\ d_1=d_2,\ d_1^*=d_2^*$, and **A** implies $\sigma_1=\sigma_2$. □[**B.**]

3. Let again $l=2k$ be even and $(d,d^*,t,\sigma)\in\mathcal{L}(D)$, where $1\le d<d^*$ and $ctd>1$. Let $x,\ y\in\mathbb{Z}$ be such that $dx^2-d^*y^2=\sigma t$. Then $\mathfrak{j}=(cdx+y\sqrt{D}\,)\mathcal{O}_{4D}$ is a reduced principal ideal of $\mathcal{O}_{4D}$ such that $\mathfrak{N}_{4D}(\mathfrak{j})=c^2dt$.

Let $(\xi_n)_{n\ge 0}$ be the sequence of complete quotients of $\sqrt{D}=\omega_{4D}$, and for $n\ge 0$ let (a_n,b_n,c_n) be the type of ξ_n. By the Theorems 2.3.5 and 5.6.9, $I(\xi_l)=\mathcal{O}_{4D}$ and $I(\xi_k)$ are the only reduced ambiguous principal ideals of $\mathcal{O}_{4D}$. Hence it follows that $\mathfrak{j}=I(\xi_k)$, and $\mathfrak{N}_{4D}(\mathfrak{j})=|\mathcal{N}(\xi_k)|=c^2dt=a_k$. By Theorem 2.3.5 we obtain

$$\mathcal{N}(\xi_k)=p_{k-1}^2-c^2dd^*q_{k-1}^2=(-1)^kc^2dt\,,\qquad c^2dt\,\varepsilon_{4D}=(p_{k-1}+q_{k-1}\sqrt{D}\,)^2$$

and

$$\varepsilon_{4D}=\frac{p_{k-1}^2+q_{k-1}^2D+2p_{k-1}q_{k-1}\sqrt{D}}{c^2dt}=(-1)^k+\frac{2d^*}{t}\,q_{k-1}^2+\frac{2p_{k-1}q_{k-1}}{c^2dt}\sqrt{D}$$

(note that $c^2dt\,|\,2p_{k-1}$). It remains to prove that $\sigma=(-1)^k$.

CASE 1: $c=2$. Then $8\,|\,D$, $t=1$, $a_k=4d\,|\,2p_{k-1}$, and therefore $p_{k-1}=2dx_1$ for some $x_1\in\mathbb{Z}$. If $y_1=q_{k-1}$, then $(p_{k-1},q_{k-1})=1$ implies $2\nmid y_1$, and it follows that $dx_1^2-d^*y_1^2=(-1)^k$. If $2\nmid x_1$, then $(d,d^*,1,(-1)^k)\in\mathcal{L}(D)$, hence $\sigma=(-1)^k$, and we are done. We assert that the case $2\,|\,x_1$ cannot occur.

Indeed, if $2\,|\,x_1$, then $x_1=2x_2$, where $x_2\in\mathbb{Z}$, and $4dx_2^2-d^*y_1^2=(-1)^k$. But this implies that $(4d,d^*,1,(-1)^k)\in\mathcal{L}(D)$, hence either $(4d,d^*,1,(-1)^k)=(d,d^*,1,\sigma)$ or $(4d,d^*,1,(-1)^k)=(d^*,4d,1,-\sigma)$, which is impossible.

CASE 2: $c=1$ and $2\nmid d$ (in particular, this occurs if $D\equiv 3\bmod 4$). As $a_k=td\,|\,2p_{k-1}$, it follows that $d\,|\,p_{k-1}$, say $p_{k-1}=dx_1$, where $x_1\in\mathbb{Z}$. If $y_1=q_{k-1}$, then it follows that $dx_1^2-d^*y_1^2=(-1)^kt$, hence $(d,d^*,t,(-1)^k)\in\mathcal{L}(D)$ and therefore $\sigma=(-1)^k$.

CASE 3: $ct=1$ and $d=2d_0$, where $d_0\in\mathbb{N}$ and $2\nmid d_0$. Since $a_k=2d_0\,|\,2p_{k-1}$, we obtain $p_{k-1}=d_0x_1$, where $x_1\in\mathbb{Z}$. If $y_1=q_{k-1}$, then $d_0x_1^2-2d^*y_1^2=2(-1)^k$, which implies that $2\,|\,x_1$. If $x_1=2x_2$, where $x_2\in\mathbb{Z}$, then $dx_2^2-d^*y_1^2=(-1)^k$, hence $(d,d^*,1,(-1)^k)\in\mathcal{L}(D)$ and therefore $\sigma=(-1)^k$.

CASE 4: $ct=1$ and $d=4^ed_0$, where e, $d_0\in\mathbb{N}$ and $4\nmid d_0$. If $D_0=d_0d^*$, then $\sigma=dx^2-d^*y^2=d_0(2^ex)^2-d^*y^2$ implies that $(d_0,d^*,1,\sigma)\in\mathcal{L}(D_0)$. Since $a_k=4^ed_0\,|\,2p_{k-1}$, it follows that $2^ed_0\,|\,2^{2e-1}d_0\,|\,p_{k-1}$, and we set $p_{k-1}=2^ed_0x_1$, where $x_1\in\mathbb{Z}$. If $y_1=q_{k-1}$, then $(p_{k-1},q_{k-1})=1$ implies $2\nmid y_1$. It follows that $d_0x_1^2-d^*y_1^2=(-1)^k$, and therefore $(d_0,d^*,1,(-1)^k)\in\mathcal{L}(D_0)$. If $d_0>1$, then $l(\sqrt{D_0}\,)$ is even, and **B** (applied with D_0 instead of D) yields $\sigma=(-1)^k$. If $d_0=1$, then $\sigma\equiv -d^*\bmod 4$. Since $2\nmid d^*y_1^2$, it follows that $2\,|\,x_1$, hence $(-1)^k\equiv -d^*\bmod 4$, and thus again $\sigma=(-1)^k$. □

As a supplement to Theorem 5.7.5 we prove that (at least for $c=1$) all solutions of a solvable equation $dx^2-d^*y^2=\pm 1$, can be derived from the continued fraction of $\sqrt{D}$.

Theorem 5.7.6. *Let $D\in\mathbb{N}$ be not a square such that $l(\sqrt{D})=2k$ is even. Let d, $d^*\in\mathbb{N}$ and $t\in\{1,2\}$ be such that*

- *$D=dd^*$, $(d,d^*)=1$, $1\le d<d^*$ and $dt\ne 1$.*
- *$t=1$ if $D\not\equiv 3\bmod 4$, and*
- *there exist $x,y\in\mathbb{Z}$ such that $dx^2-d^*y^2=(-1)^kt$ (see* Theorem 5.7.5 *).*

Let $(p_n)_{n\ge -2}$ *the sequence of partial numerators and* $(q_n)_{n\ge -2}$ *the sequence of partial denominators of* $\sqrt{D}$. *Then*

$$d \,|\, p_{k-1}\,, \quad t\varepsilon_{4D} = \Big(\frac{p_{k-1}}{d}\sqrt{d} + q_{k-1}\sqrt{d^*}\Big)^2\,,$$

and

$$\begin{aligned}\{(x,y)\in\mathbb{N}^2 \mid dx^2 - d^*y^2 = (-1)^k t\,\}\\ &= \{(x,y)\in\mathbb{N}^2 \mid (x\sqrt{d}+y\sqrt{d^*})^2 = t\varepsilon_{4D}^{2j+1} \ \ \textit{for some} \ \ j\in\mathbb{N}_0\,\}\\ &= \Big\{\Big(\frac{p_{k-1}p_{jl-1}}{d} + q_{k-1}q_{jl-1},\, p_{k-1}q_{jl-1} + q_{k-1}p_{jl-1}\Big) \ \Big|\ j\in\mathbb{N}_0\Big\}\,.\end{aligned}$$

Proof. We start with three preliminary assertions.

A. If (x,y), $(x_1,y_1)\in\mathbb{Z}^2$ and $\varepsilon\in\mathcal{O}_{4D}^\times$ are such that $dx^2-d^*y^2=(-1)^kt$ and $(x_1\sqrt{d}+y_1\sqrt{d^*})\varepsilon$, then $dx_1^2-d^*y_1^2=(-1)^kt$.

Proof of **A.** We observe that

$$\begin{aligned}dx_1^2+d^*y_1^2+2x_1y_1\sqrt{D} = (x_1\sqrt{d}+y_1\sqrt{d^*})^2 &= (x\sqrt{d}+y\sqrt{d^*})^2\varepsilon^2\\ &= (dx^2+d^*y^2+2xy\sqrt{D})\varepsilon^2.\end{aligned}$$

Taking norms, it follows that

$$\begin{aligned}(dx_1^2-d^*y_1^2)^2 = (dx_1^2+d^*y_1^2)^2 - 4x_1^2y_1^2D &= \mathcal{N}(dx_1^2+d^*y_1^2+2x_1y_1\sqrt{D})\\ &= \mathcal{N}(dx^2+d^*y^2+2xy\sqrt{D})\mathcal{N}(\varepsilon^2)\\ &= (dx^2+d^*y^2)^2-4x^2y^2D = (dx^2-d^*y^2)^2 = t^2\,,\end{aligned}$$

hence $dx_1^2-d^*y_1^2=\pm t$, and thus $dx_1^2-d^*y_1^2=(-1)^kt$ by Theorem 5.7.5. □[**A.**]

B. If $(x,y)\in\mathbb{N}^2$ and $dx^2-d^*y^2=(-1)^kt$, then $(x\sqrt{d}+y\sqrt{d^*})^2=t\varepsilon_{4D}^{2j+1}$ for some $j\in\mathbb{N}_0$.

Proof of **B.** Let $(x,y)\in\mathbb{N}^2$ be such that $dx^2-d^*y^2=(-1)^kt$. Then

$$\eta = \frac{(x\sqrt{d}+y\sqrt{d^*})^2}{t} = \frac{dx^2+d^*y^2+2xy\sqrt{D}}{t} = \frac{2d}{t}\,x^2-(-1)^k+\frac{2xy}{t}\sqrt{D}\in\mathcal{O}_{4D}\,,$$

and

$$\mathcal{N}(\eta) = \frac{(dx^2+d^*y^2)^2-4x^2y^2D}{t^2} = \frac{(dx^2-d^*y^2)^2}{t^2} = 1\,.$$

Hence $\eta\in\mathcal{O}_{4D}^\times$, and since $\eta>1$, we obtain $\eta=\varepsilon_{4D}^\nu$ for some $\nu\in\mathbb{N}$. We must prove that ν is odd. Assume to the contrary that $\nu=2j$ for some $j\in\mathbb{N}$. Then $[(x\sqrt{d}+y\sqrt{d^*})\varepsilon_{4D}^{-j}]^2=t$, and therefore

$$(x\sqrt{d}+y\sqrt{d^*})\varepsilon_{4D}^{-j} = (dx^2+d^*y^2+2xy\sqrt{D})\varepsilon_{4D}^{-j} = \pm\sqrt{t}\in\mathcal{O}_{4D}\,.$$

If $t=2$, then $D\equiv 3 \bmod 4$, and $\sqrt{2}\notin\mathbb{Q}(\sqrt{D})$. Hence it follows that $t=1$, and if $\varepsilon_{4D}^{-j}=u+v\sqrt{D}$, where u, $v\in\mathbb{N}$, then

$$(x\sqrt{d}+y\sqrt{d^*})\varepsilon_{4D}^{-j} = (ux+vyd^*)\sqrt{d}+(uy+vxd)\sqrt{d^*} = \pm 1\,.$$

If d is a square, say $d=f^2$, where $f\in\mathbb{N}$, then d^* is not a square, $(1,\sqrt{d^*})$ is linearly independent, and therefore $(ux+vyd^*)f=\pm1$. Hence $f=\pm1$ and $d=dt=1$, a contradiction. Consequently, d is not a square, we obtain

$$(ux+vy)d+(uy+vx)\sqrt{D}=\pm\sqrt{d}\in\mathbb{Q}(\sqrt{D})\,,\quad\text{whence}\quad\mathbb{Q}(\sqrt{D})=\mathbb{Q}(\sqrt{d})\,,$$

and d^* is a square. If $d^*=f^2$, where $f\in\mathbb{N}$, then the linear independence of $(1,\sqrt{d})$ implies $(uy+vxd)f=\pm1$, hence $f=\pm1$ and $d^*=1$, a contradiction. $\square$[**B.**]

C. There exists some $x_0\in\mathbb{N}$ such that $p_{k-1}=dx_0$, and if $y_0=q_{k-1}$, then

$$dx_0^2-d^*y_0^2=(-1)^kt\quad\text{and}\quad(x_0\sqrt{d}+y_0\sqrt{d^*})^2=t\varepsilon_{4D}\,.$$

Proof of **C.** Let $(x,y)\in\mathbb{N}^2$ be such that $dx^2-d^*y^2=(-1)^kt$. By **B**, there exists some $j\in\mathbb{N}_0$ such that $(x\sqrt{d}+y\sqrt{d^*})^2=t\varepsilon_{4D}^{2j+1}$. We set

$$(x\sqrt{d}+y\sqrt{d^*})\varepsilon_{4D}^{-j}=x_0\sqrt{d}+y_0\sqrt{d^*}\quad\text{with}\quad x_0,\,y_0\in\mathbb{Z}\,.$$

Then $dx_0^2-d^*y_0^2=(-1)^kt$ by **A**, and

$$(x_0\sqrt{d}+y_0\sqrt{d^*})^2=(x\sqrt{d}+y\sqrt{d^*})^2\varepsilon_{4D}^{-2j}=t\varepsilon_{4D}=tp_{l-1}+tq_{l-1}\sqrt{D}$$

by Theorem 2.3.5.4. Hence $dx_0^2+d^*y_0^2+2x_0y_0\sqrt{D}=tp_{l-1}+tq_{l-1}\sqrt{D}$, and therefore it follows that $dx_0^2+d^*y_0^2=tp_{l-1}$ and $2x_0y_0=tq_{l-1}>0$. In particular, since $x_0\sqrt{d}+y_0\sqrt{d^*}>0$, we get $x_0,\,y_0\in\mathbb{N}$. By the Theorems 5.7.5.3 and 2.3.5.1(d) we have $(-1)^ka_k=p_{k-1}^2-Dq_{k-1}^2=(-1)^kdt$, where a_k is defined there. Observing $dt=a_k$, and using Theorem 2.3.5.6(c), we obtain

$$\begin{aligned}dtp_{l-1}&=a_kp_{l-1}=p_{k-1}^2+Dq_{k-1}^2=2p_{k-1}^2-(-1)^kdt\\&=d(2dx_0^2-(-1)^kt)=2d^2x_0^2-(-1)^kdt\,,\end{aligned}$$

hence $d^2x_0^2=p_{k-1}^2$, and therefore $dx_0=p_{k-1}$. If $y_0=q_{k-1}$, then

$$dx_0^2-d^*y_0^2=\frac{(dx_0)^2-Dy_0^2}{d}=\frac{p_{k-1}^2-Dq_{k-1}^2}{d}=(-1)^kt$$

and

$$\begin{aligned}(x_0\sqrt{d}+y_0\sqrt{d^*})^2=dx_0^2+d^*y_0^2+2x_0y_0\sqrt{D}&=\frac{(dx_0)^2+Dy_0^2+dq_{l-1}\sqrt{D}}{d}\\&=\frac{p_{k-1}^2+Dq_{k-1}^2+dq_{l-1}\sqrt{D}}{d}=tp_{l-1}+tq_{l-1}\sqrt{D}=t\varepsilon_{4D}\,,\end{aligned}$$

which completes the proof of **C** and shows that

$$t\varepsilon_{4D}=\Big(\frac{p_{k-1}}{d}\sqrt{d}+q_{k-1}\sqrt{d^*}\Big)^2\,.$$

Now we can do the real proof. By **B** we obtain

$$\begin{aligned}&\{(x,y)\in\mathbb{N}^2\mid dx^2-d^*y^2=(-1)^kt\}\\&\qquad\subset\{(x,y)\in\mathbb{N}^2\mid(x\sqrt{d}+y\sqrt{d^*}\,)^2=t\varepsilon_{4D}^{2j+1}\ \text{ for some }\ j\in\mathbb{N}_0\}\,.\end{aligned}$$

To prove the reverse inclusion, let $(x,y)\in\mathbb{N}^2$ be such that $(x\sqrt{d}+y\sqrt{d^*})^2=t\varepsilon_{4D}^{2j+1}$ for some $j\in\mathbb{N}_0$. By **C**, there exists some $(x_0,y_0)\in\mathbb{N}^2$ such that $dx_0^2-d^*y_0^2=(-1)^kt$

and $t\varepsilon_{4D} = (x_0\sqrt{d} + y_0\sqrt{d^*})^2$. Hence $x\sqrt{d} + y\sqrt{d^*} = (x_0\sqrt{d} + y_0\sqrt{d^*})\varepsilon_{4D}^j$, and therefore $dx^2 - d^*y^2 = (-1)^k t$ by **A**.

To prove the second equality, let $j \in \mathbb{N}_0$, and use Theorem 2.3.5.4 and **C**. Then

$$\begin{aligned} t\varepsilon_{4D}^{2j+1} &= \varepsilon_{4D}^{2j}\Big(\frac{p_{k-1}}{d}\sqrt{d} + q_{k-1}\sqrt{d^*}\Big)^2 = \Big(\frac{(p_{jl-1} + q_{jl-1}\sqrt{D})(p_{k-1}\sqrt{d} + q_{k-1}d\sqrt{d^*})}{d}\Big)^2 \\ &= \Big(\frac{p_{k-1}p_{jl-1}}{d} + q_{k-1}q_{jl-1}d^*\Big)\sqrt{d} + (p_{k-1}q_{jl-1} + q_{k-1}p_{jl-1})\sqrt{d^*}\,. \qquad \square \end{aligned}$$

We proceed with several explicit applications of Theorem 5.7.5 . First we give a supplement to Theorem 5.7.1.

Theorem 5.7.7. *Let* $p \equiv 1 \bmod 4$ *be a prime,* $r \in \mathbb{N}$, $\Delta = 8p^r$ *and* $a,\, b \in \mathbb{N}$ *such that* $(a,b) = 1$ *and* $2p^r = a^2 + b^2$.

1. *If* $\mathcal{N}(\varepsilon_\Delta) = 1$ *and* $l(\sqrt{2p^r}\,) = 2k$, *then there exist* $x,\, y \in \mathbb{Z}$ *such that* $2x^2 - p^ry^2 = (-1)^k$, *and the Diophantine equation* $2x^2 - p^ry^2 = (-1)^{k+1}$ *is unsolvable.*
2. *If* $\mathcal{N}(\varepsilon_\Delta) = -1$, *then one of the two Diophantine equations*
$$x^2 - 2p^ry^2 = a \quad \textit{and} \quad x^2 - 2p^ry^2 = b$$
has a solution $(x,y) \in \mathbb{Z}^2$ *such that* $(x,y) = 1$, *and the Diophantine equation* $|2x^2 - p^ry^2| = 1$ *is unsolvable.*
3. *If* $p \equiv 5 \bmod 8$, *then* $\mathcal{N}(\varepsilon_\Delta) = -1$.

PROOF. 1. By Theorem 5.7.5, applied with $D = 2p^r$.

2. Assume that $\mathcal{N}(\varepsilon_\Delta) = -1$. As $|\mu(\Delta)| = 2$, Theorem 5.6.11 implies $|\mathcal{A}_\Delta| = 2$, and by Theorem 5.6.9 each ambiguous class of $\mathcal{O}_\Delta$ contains exactly one symmetric ideal. Since $\Delta = 8p^r = 4a^2 + (2b)^2 = 4b^2 + (2a)^2$, the symmetric ideals of $\mathcal{O}_\Delta$ are $\mathfrak{a} = [a, b + \sqrt{2p^r}\,]$ and $\mathfrak{b} = [b, a + \sqrt{2p^r}\,]$, and precisely one of them is principal. If $\mathfrak{a}$ is principal, then $\mathfrak{a} = \alpha\mathcal{O}_\Delta$, where $\alpha \in \mathcal{O}_\Delta^\bullet$, and since $\mathcal{N}(\varepsilon_\Delta) = -1$, we may assume that $\mathcal{N}(\alpha) = a$. If $\alpha = x + y\sqrt{2p^r}$, where $x,\, y \in \mathbb{Z}$, then $(x,y) = 1$ since $\mathfrak{a}$ is primitive, and $x^2 - 2p^ry^2 = a$. The same argument applies if $\mathfrak{b}$ is principal.

3. If $\mathcal{N}(\varepsilon_\Delta) = 1$, then 1. implies that one of the congruences $2x^2 \equiv \pm 1 \bmod p$ is solvable, and therefore either 2 or -2 is a quadratic residue modulo p, which is impossible for $p \equiv 5 \bmod 8$. $\square$

Note that in Theorem 5.7.7 both cases occur. If $p = 17$, then $\Delta = 8 \cdot 17 = 136$, $\varepsilon_\Delta = 35 + 6\sqrt{34}$, $\mathcal{N}(\varepsilon_\Delta) = 1$ and $2 \cdot 3^2 - 17 \cdot 1^2 = 1$. If $p = 29$, then $\Delta = 8 \cdot 29 = 232$, $\varepsilon_\Delta = 99 + 13\sqrt{58}$, $\mathcal{N}(\varepsilon) = -1$, $58 = 3^2 + 7^2$ and $7 = 23^2 - 58 \cdot 3^2$.

Theorem 5.7.8. *Let* $q \equiv 3 \bmod 4$ *be a prime and* $\Delta = 4q^r$ *for some odd* $r \in \mathbb{N}$.

1. $l(\sqrt{q}\,) = 2k$ *is even,* $l(\sqrt{q^r}\,) \equiv l(\sqrt{q}\,) \bmod 4$, *and there exists exactly one* $\sigma \in \{\pm 1\}$ *such that the Diophantine equation*
$$x^2 - q^ry^2 = 2\sigma \quad \textit{is soluble, namely} \quad \sigma = (-1)^k = \begin{cases} 1 & \textit{if} \quad q \equiv 7 \mod 8\,, \\ -1 & \textit{if} \quad q \equiv 3 \mod 8\,. \end{cases}$$

2. *If* $\varepsilon_\Delta = u_\Delta + v_\Delta\sqrt{q^r}$, *where* $u_\Delta,\, v_\Delta \in \mathbb{N}$, *then* $\mathcal{N}(\varepsilon_\Delta) = 1$, *and*
$$u_\Delta \equiv \begin{cases} 2 \mod 8 & \textit{if} \quad q \equiv 3 \mod 8\,, \\ 0 \mod 8 & \textit{if} \quad q \equiv 7 \mod 8\,. \end{cases}$$

Proof. $\mathcal{N}(\varepsilon_\Delta) = 1$ by Theorem 5.2.2, and therefore $l(\sqrt{q^r}\,) = 2k$ is even.

1. By Theorem 5.7.5, applied with $D = q^r$, there exists a unique $\sigma \in \{\pm 1\}$ such that the Diophantine equation
$$x^2 - q^r y^2 = 2\sigma \quad \text{has a solution} \quad (x, y) \in \mathbb{Z}^2\,.$$
More precisely, it follows that $\sigma = (-1)^k$. Hence
$$1 = \Bigl(\frac{2(-1)^k}{q}\Bigr) = (-1)^k\Bigl(\frac{2}{q}\Bigr), \quad \text{and} \quad \sigma = (-1)^k = \begin{cases} 1 & \text{if} \quad q \equiv 7 \mod 8\,, \\ -1 & \text{if} \quad q \equiv 3 \mod 8\,. \end{cases}$$
In particular, the parity $k + 2\mathbb{Z}$ of k does not depend on r.

2. Let $(p_n)_{n\ge -2}$ be the sequence of partial numerators and $(q_n)_{n \ge -2}$ the sequence of partial denominators of $\sqrt{q^r}$. Since $(1, q^r, 2, \sigma) \in \mathcal{L}(q^r)$, it follows that
$$p_{k-1}^2 - q^r q_{k-1}^2 = 2(-1)^k, \quad \text{hence} \quad 2 \nmid q_{k-1}, \quad \text{and} \quad \varepsilon_\Delta = (-1)^k + q^r q_{k-1}^2 + p_{k-1}q_{k-1}\sqrt{D}.$$
Thus we obtain $u_\Delta = (-1)^k + q^r q_{k-1}^2 \equiv (-1)^k + q^r \mod 8$, and together with 1., the assertion follows. □

Exercise 5.7.9. Let $q \equiv 3 \mod 4$ be a prime, $r \in \mathbb{N}$ and $\Delta = 8q^r$. Prove that $\mathcal{N}(\varepsilon_\Delta) = 1$, $l(\sqrt{2q}\,) = 2k$ is even, $l(\sqrt{2q^r}\,) \equiv l(\sqrt{2q}\,) \mod 4$, and there exists exactly one $\sigma \in \{\pm 1\}$ such that the Diophantine equation
$$2x^2 - q^r y^2 = \sigma \quad \text{is soluble, namely} \quad \sigma = (-1)^k = \begin{cases} 1 & \text{if} \quad q \equiv 7 \mod 8\,, \\ -1 & \text{if} \quad q \equiv 3 \mod 8\,. \end{cases}$$

Exercise 5.7.10. Let p and q be odd primes and $\Delta = 4p^r q^s$ for some odd $r,\, s \in \mathbb{N}$ such that $p^r < q^s$. Prove the following assertions:

a) If $\mathcal{N}(\varepsilon_\Delta) = -1$, then the Diophantine equation $|p^r x^2 - q^s y^2| = 1$ is unsolvable.

b) Suppose that $\mathcal{N}(\varepsilon_\Delta) = 1$ and $l(\sqrt{p^r q^s}\,) = 2k$. Then there exists precisely one $\sigma \in \{\pm 1\}$ such that the Diophantine equation $p^r x^2 - q^s y^2 = \sigma$ is solvable, namely $\sigma = (-1)^k$, and
$$\Bigl(\frac{(-1)^k p}{q}\Bigr) = \Bigl(\frac{(-1)^{k+1} q}{p}\Bigr) = 1\,.$$

Theorem 5.7.11. *Let p and q be odd primes and $\Delta = 8p^r q^s$ for some odd $r,\, s \in \mathbb{N}$. If $\mathcal{N}(\varepsilon_\Delta) = 1$, we set $l(\sqrt{2p^r q^s}) = 2k$.*

1. *Suppose that* $p \equiv 1 \mod 8$ *and* $q \equiv 5 \mod 8$.
   (a) *The Diophantine equations* $|2x^2 - p^r q^s y^2| = 1$ *and* $|2p^r x^2 - q^s y^2| = 1$ *are unsolvable.*

(b) *If* $\mathcal{N}(\varepsilon_\Delta) = 1$, *then* $l(\sqrt{2p^rq^s}) = 2k$ *is even,*

$$\Big(\frac{p}{q}\Big) = 1\,,$$

and if $\sigma \in \{\pm 1\}$, *then the Diophantine equation* $p^rx^2 - 2q^sy^2 = \sigma$ *is solvable if and only if*

$$\sigma = \begin{cases} (-1)^k & \textit{if} \ \ p^r < 2q^s\,, \\ (-1)^{k+1} & \textit{if} \ \ p^r > 2q^s\,. \end{cases}$$

(c) *If* $\mathcal{N}(\varepsilon_\Delta) = -1$, *then the Diophantine equation* $|p^rx^2 - 2q^sy^2| = 1$ *is unsolvable.*

2. *Suppose that* $p \equiv 3 \bmod 8$ *and* $q \equiv 5 \bmod 8$ (*then* $\mathcal{N}(\varepsilon_\Delta) = 1$).

(a) *The Diophantine equation* $|2x^2 - p^rq^sy^2| = 1$ *is unsolvable.*

(b) *Exactly one of the two Diophantine equations*

$$2p^rx^2 - q^sy^2 = -\Big(\frac{p}{q}\Big) \quad \textit{and} \quad p^rx^2 - 2q^sy^2 = \Big(\frac{p}{q}\Big)$$

is solvable, while the two Diophantine equations

$$2p^rx^2 - q^sy^2 = \Big(\frac{p}{q}\Big) \quad \textit{and} \quad p^rx^2 - 2q^sy^2 = -\Big(\frac{p}{q}\Big)$$

are both unsolvable.

3. *Suppose that* $p \equiv 3 \bmod 8$ *and* $q \equiv 7 \bmod 8$. *Then* $\mathcal{N}(\varepsilon_\Delta) = 1$, *and we set* $l(\sqrt{2p^rq^s}) = 2k$.

(a) *The Diophantine equations* $|2x^2 - p^rq^sy^2| = 1$ *and* $|p^rx^2 - 2q^sy^2| = 1$ *are both unsolvable.*

(b) *There exists precisely one* $\sigma \in \{\pm 1\}$ *such that the Diophantine equation* $2p^rx^2 - q^sy^2 = \sigma$ *is solvable, namely*

$$\sigma = \begin{cases} (-1)^k & \textit{if} \ \ 2p^r < q^s\,, \\ (-1)^{k+1} & \textit{if} \ \ 2p^r > q^s\,, \end{cases} \quad \textit{and} \quad (-1)^k\Big(\frac{p}{q}\Big)(q^s - 2p^r) > 0\,.$$

(c) *If* $\varepsilon_\Delta = u_\Delta + v_\Delta\sqrt{2p^rq^s}$, *then* v_Δ *is even, and*

$$\Big(\frac{p}{q}\Big) = (-1)^{v_\Delta/2}\,.$$

Proof. We apply Theorem 5.7.5 with $D = 2p^rq^s$ and note throughout that $\mathcal{N}(\varepsilon_\Delta) = 1$ and $l(\sqrt{\Delta}\,)$ is even if Δ has a prime factor $q \equiv 3 \bmod 4$. If $\mathcal{N}(\varepsilon_\Delta) = 1$, then exactly one of the six Diophantine equations

$$\text{(I)} \quad 2x^2 - p^rq^sy^2 = \pm 1\,, \quad \text{(II)} \quad 2p^rx^2 - q^sy^2 = \{\pm 1 \quad \text{(III)} \quad p^rx^2 - 2q^sy^2 = \pm 1\,,$$

is solvable. If $\mathcal{N}(\varepsilon_\Delta) = -1$, then $p \equiv q \equiv 1 \bmod 4$, and these Diophantine equations are all unsolvable.

1. (a) If $x,\, y \in \mathbb{Z}$ are such that $2x^2 - p^rq^sy^2 = \sigma \in \{\pm 1\}$, then $2x^2 \equiv \sigma \bmod q$, and therefore

$$1 = \Big(\frac{\sigma}{q}\Big) = \Big(\frac{2x^2}{q}\Big) = \Big(\frac{2}{q}\Big)\,,$$

a contradiction.

If $x,\,y\in\mathbb{Z}$ are such that $2p^rx^2-q^sy^2=\sigma\in\{\pm1\}$, then the congruences $2p^rx^2\equiv\sigma \bmod q$ and $q^sy^2\equiv\sigma \bmod p$ imply that

$$1=\Big(\frac{\sigma}{q}\Big)=\Big(\frac{2p}{q}\Big)=-\Big(\frac{p}{q}\Big)\quad\text{and}\quad 1=\Big(\frac{\sigma}{p}\Big)=\Big(\frac{q}{p}\Big)\,,$$

which contradicts the quadratic reciprocity law.

(b) By (a) and Theorem 5.7.5, there exists exactly one $\sigma\in\{\pm1\}$ such that the Diophantine equation $p^rx^2-2q^sy^2=\sigma$ is solvable, and $\sigma=(-1)^k$ holds if and only if $p^r<2q^s$. In particular, it follows that

$$1=\Big(\frac{\sigma}{q}\Big)=\Big(\frac{p^rx^2}{q}\Big)=\Big(\frac{p}{q}\Big)\,.$$

(c) By the preliminary remark.

2. (a) As in 1.(a), since ±2 is a quadratic non-residue modulo q.

(b) By the preliminary remark, exactly one of the four Diophantine equations $2p^rx^2-q^sy^2=\pm1$ and $p^rx^2-2q^sy^2=\pm1$ is solvable. Let $x,\,y\in\mathbb{Z}$ and $\sigma\in\{\pm1\}$. If $2p^rx^2-q^sy^2=\sigma$, then $\sigma\equiv-q^sy^2 \bmod p$, and therefore

$$\sigma=\Big(\frac{\sigma}{p}\Big)=-\Big(\frac{q}{p}\Big)=-\Big(\frac{p}{q}\Big)\,.$$

If $p^rx^2-2q^sy^2=\sigma$, then $\sigma\equiv-2q^sy^2 \bmod p$, and therefore

$$\sigma=\Big(\frac{\sigma}{p}\Big)=\Big(\frac{q}{p}\Big)=\Big(\frac{p}{q}\Big)\,.$$

3. (a) If $x,\,y\in\mathbb{Z}$ are such that $2x^2-p^rq^sy^2=\sigma\in\{\pm1\}$, then $2x^2\equiv\sigma \bmod p$ and $2x^2\equiv\sigma \bmod q$, which implies

$$-1=\Big(\frac{2}{p}\Big)=\Big(\frac{\sigma}{p}\Big)=\Big(\frac{\sigma}{q}\Big)=\Big(\frac{2}{q}\Big)=1\,,\quad\text{a contradiction}\,.$$

If $x,\,y\in\mathbb{Z}$ are such that $p^rx^2-2q^sy^2=\sigma\in\{\pm1\}$, then $p^rx^2\equiv\sigma \bmod q$ and $-2q^sy^2\equiv\sigma \bmod p$, which implies

$$\sigma=\Big(\frac{\sigma}{p}\Big)=\Big(\frac{-2q}{p}\Big)=\Big(\frac{q}{p}\Big)=-\Big(\frac{p}{q}\Big)=-\Big(\frac{\sigma}{q}\Big)=-\sigma\,,\quad\text{a contradiction}\,.$$

(b) There exists precisely one $\sigma\in\{\pm1\}$ such that the Diophantine equation $2p^rx^2-q^sy^2=\sigma$ is solvable, namely

$$\sigma=\begin{cases}(-1)^k & \text{if}\quad 2p^r<q^s\,,\\ (-1)^{k+1} & \text{if}\quad 2p^r>q^s\,,\end{cases}\quad\text{and}\quad(-1)^k\Big(\frac{p}{q}\Big)(q^s-2p^r)>0\,.$$

(c) Let $(p_n)_{n\ge-2}$ be the sequence of partial numerators and $(q_n)_{n\ge-2}$ the sequence of partial denominators of $\sqrt{2p^rq^s}$.

CASE 1: $2p^r<q^s$. Then $(2p^r,q^s,1,(-1)^k)\in\mathcal{L}(2p^rq^s)$, and therefore we obtain $p_{k-1}^2-2p^rq^sq_{k-1}^2=(-1)^k2p^r$, $2\,|\,p_{k-1}$, $2\nmid q_{k-1}$,

$$\varepsilon_\Delta=(-1)^k+2q^sq_{k-1}^2+\frac{p_{k-1}q_{k-1}}{p^r}\sqrt{2p^rq^s}\,,\quad\text{and}\quad \mathsf{v}_2(v_\Delta)=\mathsf{v}_2\Big(\frac{p_{k-1}q_{k-1}}{p^r}\Big)\ge1\,.$$

Since $p_{k-1}^2 = 2p^r\,[(-1)^k + q^s q_{k-1}^2\,] \equiv 2\,[1-(-1)^k\,] \bmod 8$, it follows that $4\,|\,v_\Delta$ if and only if $2\,|\,k$, and therefore

$$\Big(\frac{p}{q}\Big) = (-1)^k = (-1)^{v_\Delta/2}\,.$$

CASE 2: $q^s < 2p^r$. Then $(q^s, 2p^r, 1, (-1)^k) \in \mathcal{L}(2p^r q^s)$, and therefore we obtain $p_{k-1}^2 - 2p^r q^s q_{k-1}^2 = (-1)^k q^s$, $2 \nmid p_{k-1}$,

$$\varepsilon_\Delta = (-1)^k + 4p^r q_{k-1}^2 + \frac{2p_{k-1}q_{k-1}}{q^s}\sqrt{2p^r q^s}\,,$$

and

$$\mathsf{v}_2(v_\Delta) = \mathsf{v}_2\Big(\frac{2p_{k-1}q_{k-1}}{q^s}\Big) = \mathsf{v}_2(q_{k-1}) + 1 \ge 1\,.$$

Since $1 \equiv p_{k-1}^2 \equiv q^s\,[\,2p^r q_{k-1}^2 + (-1)^k\,] \equiv 2q_{k-1}^2 - (-1)^k \bmod 8$, it follows that $4\,|\,v_\Delta$ if and only if $2 \nmid k$, and therefore

$$\Big(\frac{p}{q}\Big) = (-1)^{k-1} = (-1)^{v_\Delta/2}\,. \qquad \square$$

We proceed with a counterpart to the Theorems 5.7.5 and 5.7.6 for discriminants $\Delta \equiv 1 \bmod 4$.

Theorem 5.7.12. *Let $\Delta \in \mathbb{N}$ be not a square, $\Delta \equiv 1 \bmod 4$, $l = l(\omega_\Delta)$ the period length of ω_Δ and $l^* = l(\sqrt{\Delta}\,)$ the period length of $\sqrt{\Delta}$. Let $\mathcal{L}_0(\Delta)$ be the set of all triples (d, d^*, σ) such that*

> *$d,\ d^* \in \mathbb{N}$, $(d, d^*) = 1$, $\Delta = dd^*$, $\sigma \in \{\pm 1\}$, and there exist $x,\ y \in \mathbb{Z}$ such that $dx^2 - d^*y^2 = 4\sigma$.*

Then $|\mathcal{L}_0(\Delta)| = 4$, and the structure of $\mathcal{L}_0(\Delta)$ is as follows.

1. *If l is odd, then $\mathcal{L}_0(\Delta) = \{(1, \Delta, \pm 1),\ (\Delta, 1, \pm 1)\,\}$.*
2. *If $l = 2k$ is even, then $\mathcal{L}_0(\Delta) = \{(1, \Delta, 1),\ (\Delta, 1, -1),\ (d, d^*, \sigma),\ (d^*, d, -\sigma)\}$, where $(d, d^*, \sigma) \notin \{(1, \Delta, -1),\ (\Delta, 1, 1)\,\}$.*
3. *Let $l = 2k$ be even, $(d, d^*, \sigma) \in \mathcal{L}_0(\Delta)$ and $1 < d < d^*$. Let $(p_n)_{n \ge -2}$ be the sequence of partial numerators, $(q_n)_{n \ge -2}$ the sequence of partial denominators of ω_Δ, and set $p_n' = 2p_n - q_n$ for all $n \ge -2$. Then the following assertions hold:*
    - (a) *$\sigma = (-1)^k$, $p_{k-1}' = ds_k$, $ds_k^2 - d^* q_{k-1}^2 = 4(-1)^k$, and*

      $$\varepsilon_\Delta = \Big(\frac{s_k\sqrt{d} + q_{k-1}\sqrt{d^*}}{2}\Big)^2 = (-1)^k + \frac{d^* q_{k-1}^2 + q_{k-1}s_k\sqrt{\Delta}}{2}\,,$$

    - (b) *$\varepsilon_\Delta \notin O_{4\Delta}$ if and only if there exist $x,\ y \in \mathbb{Z}$ such that $|dx^2 - d^*y^2| = 4$ and $(x, y) = 1$.*

(c) *We have*

$$\begin{aligned}&\{(x,y)\in\mathbb{N}^2 \mid dx^2-d^*y^2=4(-1)^k\,\}\\ &\quad=\{(x,y)\in\mathbb{N}^2 \mid (x\sqrt{d}+y\sqrt{d^*})^2=4\varepsilon_\Delta^{2j+1}\ \ \textit{for some}\ \ j\in\mathbb{N}_0\,\}\\ &\quad=\Big\{\Big(\frac{p'_{jl-1}s_k+q_{jl-1}q_{k-1}d^*}{2},\ \frac{q_{jl-1}s_kd+p'_{jl-1}q_{k-1}}{2}\Big)\ \Big|\ j\in\mathbb{N}_0\Big\}\,.\end{aligned}$$

(d) *There exist* $x_1,\ y_1\in\mathbb{Z}$ *such that* $dx_1^2-d^*y_1^2=\sigma$*. In particular, if* l *is even, then* $l\equiv l^* \bmod 4$*.*

Proof. As the proofs of 1. and 2. are completely analogous to that of Theorem 5.7.5, we leave them to the reader and limit ourselves to the proof of 3.

3. Let $l=2k$ be even and $(d,d^*,\sigma)\in\mathcal{L}_0(\Delta)$, where $1<d<d^*$. Let $x,\ y\in\mathbb{Z}$ be such that $dx^2-d^*y^2=4\sigma$. Then

$$\mathfrak{j}=\Big(\frac{dx+y\sqrt{\Delta}}{2}\Big)\mathcal{O}_\Delta=\Big[\,d,\ \frac{d+\sqrt{\Delta}}{2}\,\Big]$$

is a reduced principal ideal of $\mathcal{O}_\Delta$ such that $\mathfrak{N}(\mathfrak{j})=d$ by Theorem 5.7.2.2.

Let $(\xi_n)_{n\ge0}$ be the sequence of complete quotients of ω_Δ, and for $n\ge0$ let (a_n,b_n,c_n) be the type of ξ_n. As in the proof of Theorem 5.7.5, the ideals $I(\xi_l)=\mathcal{O}_\Delta$ and $I(\xi_k)$ are the only reduced ambiguous principal ideals of $\mathcal{O}_{4D}$. Hence it follows that $\mathfrak{j}=I(\xi_k)$ and $\mathfrak{N}_\Delta(\mathfrak{j})=|\mathcal{N}(\xi_k)|=d=a_k$.

(a) By Theorem 2.3.5 [6(a), 1(d) and 6(d)], we get $p'_{k-1}=2p_{k-1}-q_{k-1}=ds_k$, $4(-1)^kd=d^2s_k^2-dd^*q_{k-1}^2$, and

$$d\varepsilon_\Delta=\Big(p_{k-1}-q_{k-1}\frac{1-\sqrt{\Delta}}{2}\Big)^2=\Big(\frac{ds_k+q_{k-1}\sqrt{\Delta}}{2}\Big)^2.$$

Hence $4(-1)^k=ds_k^2-d^*q_{k-1}^2$, and

$$\begin{aligned}\varepsilon_\Delta&=\Big(\frac{s_k\sqrt{d}+q_{k-1}\sqrt{d^*}}{2}\Big)^2=\frac{ds_k^2+d^*q_{k-1}^2+2s_kq_{k-1}\sqrt{\Delta}}{4}\\ &=(-1)^k+\frac{d^*q_{k-1}^2+q_{k-1}s_k\sqrt{\Delta}}{2}\,.\end{aligned}$$

In particular, $(d,d^*,(-1)^k)\in\mathcal{L}_0(\Delta)$, and by **A** it follows that $(d,d^*,\sigma)\in\mathcal{L}_0(\Delta)$ if and only if $\sigma=(-1)^k$.

(b) By (a) it follows that $\varepsilon_\Delta\notin\mathcal{O}_{4\Delta}$ if and only if $2\nmid q_{k-1}$, and in this case $(x,y)=(s_k,q_{k-1})$ is a solution of the Diophantine equation $|dx^2-d^*y^2|=4$ such that $(x,y)=1$. Conversely, if $x,\ y\in\mathbb{Z}$, $(x,y)=1$ and $dx^2-d^*y^2=\sigma\in\{\pm1\}$, then

$$\varepsilon=\frac{2\sigma+d^*y^2+xy\sqrt{\Delta}}{2}\in\mathcal{O}_\Delta^\times\setminus\mathcal{O}_{4\Delta}\,.$$

(c) Let $(x,y)\in\mathbb{N}^2$ be such that $dx^2-d^*y^2=4(-1)^k$. Then it follows that $dx^2+d^*y^2\equiv 2xy \bmod 4$, hence

$$\eta=\Big(\frac{x\sqrt{d}+y\sqrt{d^*}}{2}\Big)^2=\frac{dx^2+d^*y^2+2xy\sqrt{\Delta}}{4}\in\mathcal{O}_\Delta\,,$$

and since

$$\mathcal{N}(\eta)=\frac{(dx^2+d^*y^2)^2-4x^2y^2\Delta}{16}=\frac{(dx^2-d^*y^2)^2}{16}=1 \quad\text{and}\quad \eta>1\,,$$

we get $\eta\in\mathcal{O}_\Delta^\times$ and $\eta=\varepsilon_\Delta^\nu$ for some $\nu\in\mathbb{N}$. We assert that ν is odd. Assume to the contrary that $\nu=2j$ for some $j\in\mathbb{N}$. Then $[(x\sqrt{d}+y\sqrt{d^*})\varepsilon_\Delta^{-j}]^2=4$, and therefore

$$(x\sqrt{d}+y\sqrt{d^*})\varepsilon_\Delta^{-j}=(dx^2+d^*y^2+2xy\sqrt{\Delta})\varepsilon_\Delta^{-j}=\pm 2\,.$$

If $2\varepsilon_\Delta^{-j}=u+v\sqrt{\Delta}$, where $u,\ v\in\mathbb{N}$ and $u\equiv v \mod 2$, then

$$2(x\sqrt{d}+y\sqrt{d^*})\varepsilon_\Delta^{-j}=(ux+vyd^*)\sqrt{d}+(uy+vxd)\sqrt{d^*}=\pm 4\,.$$

If d is a square, say $d=f^2$, where $f\in\mathbb{N}$, then d^* is not a square, $(1,\sqrt{d^*})$ is linearly independent, and therefore $(ux+vyd^*)f=\pm 4$. Since f is odd, we obtain $f=\pm 1$ and $d=1$, a contradiction. Hence d is not a square,

$$(ux+vy)d+(uy+vx)\sqrt{\Delta}=\pm\sqrt{d}\in\mathbb{Q}(\sqrt{\Delta})\,,\quad \mathbb{Q}(\sqrt{\Delta})=\mathbb{Q}(\sqrt{d})\,,$$

and therefore d^* is a square. If $d^*=f^2$, where $f\in\mathbb{N}$, then the linear independence of $(1,\sqrt{d})$ implies $(uy+vxd)f=\pm 4$, hence $f=\pm 1$ as f is odd, and $d^*=1$, a contradiction.

Up to now, we have proved that

$$\begin{aligned}&\{(x,y)\in\mathbb{N}^2 \mid dx^2-d^*y^2=4(-1)^k\,\}\\ &\qquad\subset\{(x,y)\in\mathbb{N}^2 \mid (x\sqrt{d}+y\sqrt{d^*}\,)^2=4\varepsilon_\Delta^{2j+1}\ \text{ for some }\ j\in\mathbb{N}_0\,\}\,.\end{aligned}$$

To prove the reverse inclusion, let $(x,y)\in\mathbb{N}^2$ be such that $(x\sqrt{d}+y\sqrt{d^*})^2=4\varepsilon_\Delta^{2j+1}$ for some $j\in\mathbb{N}_0$. By (a), we obtain

$$\begin{aligned}dx^2+d^*y^2+2xy\sqrt{\Delta}&=(x\sqrt{d}+y\sqrt{d^*})^2=(s_k\sqrt{d}+q_{k-1}\sqrt{d^*})^2\varepsilon_\Delta^{2j}\\&=(ds_k^2+d^*q_{k-1}^2+2s_kq_{k-1}\sqrt{\Delta})\varepsilon_\Delta^{2j}\,.\end{aligned}$$

Taking norms, it follows that

$$\begin{aligned}(dx^2-d^*y^2)^2&=(dx^2+d^*y^2)^2-4x^2y^2\Delta=[\,(ds_k^2-d^*q_{k-1}^2)^2-4s_k^2q_{k-1}^2\Delta\,]\mathcal{N}(\varepsilon_\Delta^{2j})\\&=(ds_k^2-d^*q_{k-1}^2)^2=16\,,\end{aligned}$$

hence $dx_1^2-d^*y_1^2=4\sigma$, where $\sigma\in\{\pm 1\}$, and by (a) we obtain $\sigma=(-1)^k$.

To prove the second equality, we use Theorem 2.3.5.4 and obtain

$$\begin{aligned}4\varepsilon_\Delta^{2j+1}&=\varepsilon_\Delta^{2j}(s_k\sqrt{d}+q_{k-1}\sqrt{d^*})^2=\Big[\Big(p_{jl-1}-q_{jl-1}\frac{1-\sqrt{\Delta}}{2}\Big)(s_k\sqrt{d}+q_{k-1}\sqrt{d^*})\Big]^2\\&=\Big(\frac{(p'_{jl-1}+q_{jl-1}\sqrt{\Delta})(s_k\sqrt{d}+q_{k-1}\sqrt{d^*})}{2}\Big)^2\\&=\frac{p'_{jl-1}s_k+q_{jl-1}q_{k-1}d^*}{2}\sqrt{d}\ +\ \frac{q_{jl-1}s_kd+p'_{jl-1}q_{k-1}}{2}\sqrt{d^*}\,.\end{aligned}$$

(d) Suppose that $(d,d^*,\sigma)\in\mathcal{L}_0(\Delta)$ and $x,\ y\in\mathbb{Z}$ are such that $dx^2-d^*y^2=4\sigma$. If $x\equiv y\equiv 0 \mod 2$, we set $x=2x_1,\ \ y=2y_1$, and we obtain $dx_1^2-d^*y_1^2=\sigma$. Thus assume now that $x \equiv y \equiv 1 \bmod 2$. Then we set

$$x_1 = \frac{(dx^2 - 3\sigma)x}{2} \quad \text{and} \quad y_1 = \frac{(dx^2 - \sigma)y}{2}\,,$$

and we assert that $dx_1^2 - d^*y_1^2 = \sigma$. For the proof, we start with the identity

$$64\sigma d^3 = (d^2x^2 - \Delta y^2)^3 = [dx(d^2x^2 + 3\Delta y^2)]^2 - \Delta[y(3d^2x^2 + \Delta y^2)]^2\,.$$

Now we find

$$\begin{aligned} dx(d^2x^2 + 3\Delta y^2) &= dx[4d^2x^2 - 3(d^2x^2 - \Delta y^2)] = dx(4d^2x^2 - 12d\sigma) \\ &= 4d^2x(dx^2 - 3\sigma) = 8d^2x_1 \end{aligned}$$

and

$$\begin{aligned} y(3d^2x^2 + \Delta y^2) &= y[4d^2x^2 - (d^2x^2 - \Delta y^2)] = y(4d^2x^2 - 4d\sigma) \\ &= 4dy(dx^2 - \sigma) = 8dy_1\,. \end{aligned}$$

It follows that $64\sigma d^3 = 64d^4x_1^2 - 64d^2y_1^2\Delta$, and therefore $\sigma = dx_1^2 - d^*y_1^2$.

Suppose now that l is even. Then there exists some $(d, d^*, \sigma) \in \mathcal{L}_0(\Delta)$ such that $1 < d < d^*$. By Theorem 5.7.5 it follows that $(d, d^*, 1, \sigma) \in \mathcal{L}(\Delta)$, hence l^* is even, and if $l^* = 2k^*$, then $\sigma = (-1)^k = (-1)^{k^*}$, which implies $l \equiv l^* \bmod 4$. □

5.8. Prime ideals and multiplicative ideal theory

We investigate the behavior of prime ideals in quadratic orders. Although some of the results hold in a more general setting and are well known from commutative ring theory or elementary algebraic number theory, we give ad hoc proofs valid in our special case. The most interesting assertion in the subsequent Theorem 5.8.1 is the prime ideal factorization of ideals coprime to the conductor.

After that, we deal with factorization properties, the decomposition law for primes and the structure of the residue class groups of quadratic orders.

Theorem 5.8.1. *Let Δ be a quadratic discriminant.*

1. *If $\mathfrak{p}$ is a non-zero prime ideal of $\mathcal{O}_\Delta$, then $\mathfrak{p}$ is a maximal ideal, $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for some prime p, and p is the only prime lying in $\mathfrak{p}$.*
2. *Every proper ideal of $\mathcal{O}_\Delta$ is contained in some prime ideal.*
3. *If $\mathfrak{p}$ is an ideal of $\mathcal{O}_\Delta$ such that $\mathfrak{N}_\Delta(\mathfrak{p})$ is a prime, then $\mathfrak{p}$ is an $\mathcal{O}_\Delta$-primitive prime ideal.*
4. *Let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}_\Delta$ such that $(\mathfrak{N}_\Delta(\mathfrak{a}), f_\Delta) = 1$. Then $\mathfrak{a}$ is a product of prime ideals of $\mathcal{O}_\Delta$ in a unique way (apart from the order of the factors). Moreover, if $\mathfrak{a} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$, where $r \in \mathbb{N}_0$ and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are prime ideals, then $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are invertible, and $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ is the set of all prime ideals of $\mathcal{O}_\Delta$ containing $\mathfrak{a}$.*

   In particular, if Δ is a fundamental discriminant, then every non-zero ideal of $\mathcal{O}_\Delta$ is a product of prime ideals in an essentially unique way.

Proof. 1. Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_\Delta$. Then $\mathcal{O}_\Delta/\mathfrak{p}$ is a finite integral domain, hence a field, and thus $\mathfrak{p}$ is a maximal ideal. As $\mathfrak{p} \cap \mathbb{Z}$ is a non-zero prime ideal of $\mathbb{Z}$, we obtain $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ for some prime p, and if $q \in \mathfrak{p}$ is any prime, then $q\mathbb{Z} \subset \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ implies $p = q$.

2. Let $\mathfrak{a}$ be a proper ideal of $\mathcal{O}_\Delta$. We may assume that $\mathfrak{a} \neq \mathbf{0}$, and we use induction on $\mathfrak{N}_\Delta(\mathfrak{a})$. If $\mathfrak{a}$ is maximal, there is nothing to do. Otherwise there is an ideal $\mathfrak{b}$ of $\mathcal{O}_\Delta$ such that $\mathfrak{a} \subsetneq \mathfrak{b} \subsetneq \mathcal{O}_\Delta$, hence $\mathfrak{N}_\Delta(\mathfrak{b}) < \mathfrak{N}_\Delta(\mathfrak{a})$. By the induction hypothesis, $\mathfrak{b}$ (and thus also $\mathfrak{a}$) is contained in some prime ideal of $\mathcal{O}_\Delta$.

3. Let $\mathfrak{p}$ be an ideal of $\mathcal{O}_\Delta$ such that $\mathfrak{N}_\Delta(\mathfrak{p})$ is a prime. If $\mathfrak{p}$ is not $\mathcal{O}_\Delta$-primitive, then $e^{-1}\mathfrak{p} \subset \mathcal{O}_\Delta$ for some integer $e \geq 2$ and thus $e^2 \mid \mathfrak{N}_\Delta(\mathfrak{p})$, a contradiction. If $\mathfrak{p}$ is not a prime ideal, then 2. implies that there is an ideal $\mathfrak{a}$ of $\mathcal{O}_\Delta$ such that $\mathfrak{p} \subsetneq \mathfrak{a} \subsetneq \mathcal{O}_\Delta$, hence $\mathfrak{N}_\Delta(\mathfrak{a}) \mid \mathfrak{N}_\Delta(\mathfrak{p})$ and $1 < \mathfrak{N}_\Delta(\mathfrak{a}) < \mathfrak{N}_\Delta(\mathfrak{p})$, again a contradiction.

4. Recall from Corollary 5.4.3 that every non-zero ideal $\mathfrak{c}$ of $\mathcal{O}_\Delta$ satisfying $(\mathfrak{N}_\Delta(\mathfrak{c}), f_\Delta) = 1$ is $\mathcal{O}_\Delta$-invertible. In particular, $\mathfrak{a}$ itself and every ideal $\mathfrak{c}$ of $\mathcal{O}_\Delta$ containing $\mathfrak{a}$ is $\mathcal{O}_\Delta$-invertible.

After this preliminary remark we use induction on $\mathfrak{N}_\Delta(\mathfrak{a})$, and we may assume that $\mathfrak{a} \subsetneq \mathcal{O}_\Delta$. By 2. there exists a prime ideal $\mathfrak{p}_1$ of $\mathcal{O}_\Delta$ such that $\mathfrak{a} \subset \mathfrak{p}_1$. As $\mathfrak{p}_1$ is $\mathcal{O}_\Delta$-invertible, Theorem 5.3.5 implies that there exists an ideal $\mathfrak{b}$ of $\mathcal{O}_\Delta$ such that $\mathfrak{a} = \mathfrak{p}_1\mathfrak{b}$, and then $\mathfrak{a} \subsetneq \mathfrak{b}$. Indeed, obviously $\mathfrak{a} \subset \mathfrak{b}$, but $\mathfrak{a} = \mathfrak{b}$ implies $\mathfrak{p}_1 = \mathcal{O}_\Delta$, since $\mathfrak{a}$ is $\mathcal{O}_\Delta$-invertible. Hence $\mathfrak{N}_\Delta(\mathfrak{b}) < \mathfrak{N}_\Delta(\mathfrak{a})$, and the induction hypothesis implies that $\mathfrak{b} = \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_n$ for some $n \in \mathbb{N}$ and prime ideals $\mathfrak{p}_2, \ldots, \mathfrak{p}_n$. Consequently, $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_n$.

To prove uniqueness, assume that $\mathfrak{a} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_n = \mathfrak{p}_1' \cdot \ldots \cdot \mathfrak{p}_m'$ with $n, m \in \mathbb{N}$ and prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n, \mathfrak{p}_1', \ldots, \mathfrak{p}_m'$ of $\mathcal{O}_\Delta$. We proceed by induction on n, and note that $n = 1$ if and only if $m = 1$, and in this case the assertion is obvious. Thus suppose that $n \geq 2$. Since $\mathfrak{a} = \mathfrak{p}_1' \cdot \ldots \cdot \mathfrak{p}_m' \subset \mathfrak{p}_1$, there is some $j \in [1, m]$ such that $\mathfrak{p}_j' \subset \mathfrak{p}_1$, and, after renumbering if necessary, we may assume that $\mathfrak{p}_1' \subset \mathfrak{p}_1$. By 1. we obtain $\mathfrak{p}_1' = \mathfrak{p}_1$, hence $\mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_n = \mathfrak{p}_2' \cdot \ldots \cdot \mathfrak{p}_m'$, and by the induction hypothesis it follows that $m = n$ and $\mathfrak{p}_j = \mathfrak{p}_j'$ for all $j \in [2, n]$.

If $\mathfrak{a} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$ with prime ideals $\mathfrak{p}_1, \ldots \mathfrak{p}_r$ of $\mathcal{O}_\Delta$, then $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ are $\mathcal{O}_\Delta$-invertible, $\mathfrak{a} \subset \mathfrak{p}_i$ for all $i \in [1, r]$, and if $\mathfrak{p}$ is any prime ideal of $\mathcal{O}_\Delta$ containing $\mathfrak{a}$, then $\mathfrak{p}_i \subset \mathfrak{p}$ and thus $\mathfrak{p}_i = \mathfrak{p}$ for some $i \in [1, r]$. Hence $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ is the set of all prime ideals of $\mathcal{O}_\Delta$ which contain $\mathfrak{a}$. □

Exercise 5.8.2. Let Δ be a quadratic discriminant, $\mathfrak{a}$ an $\mathcal{O}_\Delta$-invertible fractional $\mathcal{O}_\Delta$-ideal and $\mathfrak{p}$ a non-zero prime ideal of $\mathcal{O}_\Delta$. Prove that $\mathfrak{p}\mathfrak{a} \subsetneq \mathfrak{a}$, and that there is no fractional $\mathcal{O}_\Delta$-ideal lying strictly between $\mathfrak{p}\mathfrak{a}$ and $\mathfrak{a}$.

Exercise 5.8.3. Let Δ be a quadratic discriminant such that $h_\Delta = 1$. Prove that every $\alpha \in D^\bullet$ such that $(\mathcal{N}(\alpha), f_\Delta) = 1$ is a product of prime elements of $\mathcal{O}_\Delta$.

Next we have a closer look at factorization properties and the behavior of primes (see Section A.8 for the relevant definitions and elementary results of factorization theory). In particular, we prove a criterion for unique factorization (Theorem 5.8.6) and present the decomposition laws for primes in an explicit form (Theorem 5.8.8).

Recall the definition of the quadratic symbol Q_Δ (see Section 3.5) : If Δ is a quadratic discriminant and p is a prime, then

$$\mathsf{Q}_\Delta(p) = \Big(\frac{\Delta}{p}\Big) = \begin{cases} 1 & \text{if } \ p \nmid \Delta \ \text{ and } \Delta \text{ is a quadratic residue modulo } 4p, \\ -1 & \text{if } \ p \nmid \Delta \ \text{ and } \Delta \text{ is a quadratic non-residue modulo } 4p, \\ 0 & \text{if } \ p \,|\, \Delta\,. \end{cases}$$

Theorem 5.8.4. *Let Δ be a quadratic discriminant.*

1. *$\mathcal{O}_\Delta$ is atomic.*
2. *A prime p is a prime element of $\mathcal{O}_\Delta$ if and only if $\mathsf{Q}_\Delta(p) = -1$.*
3. *Every prime dividing f_Δ is an atom but not a prime element of $\mathcal{O}_\Delta$.*

Proof. 1. We must prove that every $a \in \mathcal{O}_\Delta^\bullet$ has a factorization $a = eu_1 \cdot \ldots \cdot u_k$, where $e \in \mathcal{O}_\Delta^\times$, $k \in \mathbb{N}_0$ and $u_1, \ldots, u_k \in \mathcal{O}_\Delta$ are atoms.

We proceed by induction on $|\mathcal{N}(a)|$. If $a \in \mathcal{O}_\Delta^\times$ or if a is an atom, there is nothing to do. Thus suppose that $a \in \mathcal{O}_\Delta^\bullet \setminus \mathcal{O}_\Delta^\times$ is not an atom. Then $a = bc$, where $b,\, c \in \mathcal{O}_\Delta^\bullet \setminus \mathcal{O}_\Delta^\times$, and $\mathcal{N}(a) = \mathcal{N}(b)\mathcal{N}(c)$ implies $1 < |\mathcal{N}(b)| < |\mathcal{N}(a)|$ and $1 < |\mathcal{N}(c)| < |\mathcal{N}(a)|$. By the induction hypothesis, both b and c have a factorization of the desired form, and thus the same is true for a.

2. Let p be a prime.

CASE 1 : $\mathsf{Q}_\Delta(p) = -1$. We prove that $p\mathcal{O}_\Delta$ is a prime ideal. Let $x,\, y \in \mathcal{O}_\Delta$ be such that $xy \in p\mathcal{O}_\Delta$, say $xy = p\alpha$ for some $\alpha \in \mathcal{O}_\Delta$. Then it follows that $\mathcal{N}(x)\mathcal{N}(y) = \mathcal{N}(xy) = \mathcal{N}(p)\mathcal{N}(\alpha) = p^2\mathcal{N}(\alpha)$, hence $p \,|\, \mathcal{N}(x)\mathcal{N}(y)$, and we may assume that $p \,|\, \mathcal{N}(x)$. Suppose that

$$x = \frac{u + v\sqrt{\Delta}}{2}\,, \quad \text{where} \quad u,\, v \in \mathbb{Z}\,,\ u \equiv v\Delta \mod 2 \quad \text{and} \quad \mathcal{N}(x) = \frac{u^2 - v^2\Delta}{4}\,.$$

Hence it follows that $4p \,|\, u^2 - v^2\Delta$. If $p \ne 2$, then Δ is a quadratic non-residue modulo p, hence $u \equiv v \equiv 0 \mod p$ and $x \in p\mathcal{O}_\Delta$. If $p = 2$, then $\Delta \equiv 5 \mod 8$ and $u^2 - v^2\Delta \equiv u^2 - 5v^2 \equiv 0 \mod 8$. But then we obtain either $u \equiv v \equiv 0 \mod 4$ or $u \equiv v \equiv 2 \mod 4$, and in both cases it follows that $x \in 2\mathcal{O}_\Delta$.

CASE 2 : $\mathsf{Q}_\Delta(p) = 1$. By Theorem 3.5.5.4 there exist $x,\, u \in \mathbb{Z}$ such that $x^2 - \Delta = 4pu$. In particular, $x \equiv \Delta \mod 2$, and therefore

$$\frac{x \pm \sqrt{\Delta}}{2} \in \mathcal{O}_\Delta\,, \quad \frac{x - \sqrt{\Delta}}{2}\,\frac{x + \sqrt{\Delta}}{2} = pu \in p\mathcal{O}_\Delta\,, \quad \text{but} \quad \frac{x \pm \sqrt{\Delta}}{2} \notin p\mathcal{O}_\Delta\,.$$

Hence p is not a prime element of $\mathcal{O}_\Delta$.

CASE 3 : $\mathsf{Q}_\Delta(p) = 0$. If $p \ne 2$, then $p \,|\, \Delta$, hence $\Delta = (\sqrt{\Delta})^2 \in p\mathcal{O}_\Delta$, but $\sqrt{\Delta} \notin p\mathcal{O}_\Delta$. Hence p is not a prime element of $\mathcal{O}_\Delta$.

Thus assume that $p = 2$. Then $\Delta = 4D$, where $D \in \mathbb{Z}$, and $\mathcal{O}_\Delta = \mathbb{Z}[\sqrt{D}\,]$. If $2 \,|\, D$, then (as before) $D = (\sqrt{D})^2 \in 2\mathcal{O}_\Delta$, but $\sqrt{D} \notin \mathcal{O}_\Delta$. If $2 \nmid D$, then $1 - D = (1 + \sqrt{D})(1 - \sqrt{D}) \in 2\mathcal{O}_\Delta$, but $1 \pm \sqrt{D} \notin 2\mathcal{O}_\Delta$. Hence 2 is not a prime element of $\mathcal{O}_\Delta$.

3. Assume to the contrary that some prime p dividing f_Δ is not an atom of $\mathcal{O}_\Delta$, say $f_\Delta = pf$, where $f \in \mathbb{N}$, and $p = xy$ for some $x,\, y \in \mathcal{O}_\Delta \setminus \mathcal{O}_\Delta^\times$. Then $p^2 = \mathcal{N}(p) = |\mathcal{N}(x)|\,|\mathcal{N}(y)|$, $|\mathcal{N}(x)| \ne 1$ and $|\mathcal{N}(y)| \ne 1$. Hence $|\mathcal{N}(x)| = p$, and if

$$x = \frac{u + v\sqrt{\Delta}}{2}\,, \text{ where } u,\, v \in \mathbb{Z} \text{ and } u \equiv v\Delta \bmod 2\,, \text{ then } 4p = |u^2 - v^2\Delta|\,.$$

If Δ_0 is the fundamental discriminant associated with Δ, then $\Delta = p^2f^2\Delta_0$, hence $p \,|\, u$, which implies $p^2 \,|\, 4p$ and thus $p = 2$. If $u = 2u_0$, then $2 = |u_0^2 - v^2f^2\Delta_0|$, but this is impossible since $v^2f^2\Delta_0 \equiv 0$ or $1 \bmod 4$.

If p is a prime dividing f_Δ, then $\mathsf{Q}_\Delta(p) = 0$, and thus p is not a prime element of $\mathcal{O}_\Delta$. □

Exercise 5.8.5. Let $\Delta < 0$ be a quadratic discriminant, and

$$\alpha = \frac{a + b\sqrt{\Delta}}{2} \in \mathcal{O}_\Delta^\bullet\,, \quad \text{where } a,\, b \in \mathbb{Z} \text{ and } a \equiv b\Delta \bmod 2\,.$$

Suppose that $4\mathcal{N}(\alpha) < \Delta^2$, and $(a,b) = 1$. Prove that α is an atom of $\mathcal{O}_\Delta$.

Theorem 5.8.6. *Let Δ be a quadratic discriminant. Then the following assertions are equivalent:*

(a) *$\mathcal{O}_\Delta$ is a principal ideal domain.*

(b) *$\mathcal{O}_\Delta$ is factorial.*

(c) *Δ is a fundamental discriminant, and $h_\Delta = 1$.*

In particular, the maximal order $\mathcal{O}_K$ of a quadratic number field K is factorial if and only if $h_K = 1$.

Proof. (a) ⇒ (b) By Theorem A.8.3.1.

(b) ⇒ (c) If Δ is not a fundamental discriminant and p is a prime dividing f_Δ, then Theorem 5.8.4 implies that p is an atom but not a prime element of $\mathcal{O}_\Delta$. Hence $\mathcal{O}_\Delta$ is not factorial (see Theorem A.8.1.3).

Thus let Δ be a fundamental discriminant. It suffices to prove that every prime ideal of $\mathcal{O}_\Delta$ is principal. Indeed, by Theorem 5.8.1.4, every non-zero ideal of $\mathcal{O}_\Delta$ is a product of prime ideals, hence principal, and thus $h_\Delta = 1$.

Thus let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_\Delta$ and $a \in \mathfrak{p}^\bullet$. Then $a = \pi_1 \cdot \ldots \cdot \pi_n$, where $n \in \mathbb{N}$ and $\pi_1, \ldots, \pi_n \in \mathcal{O}_\Delta$ are prime elements. Hence there is some $i \in [1,n]$ such that $\pi_i \in \mathfrak{p}$. Since $\pi_i\mathcal{O}_\Delta \subset \mathfrak{p}$ and $\pi_i\mathcal{O}_\Delta$ is a maximal ideal by Theorem 5.8.1.1, it follows that $\mathfrak{p} = \pi_i\mathcal{O}_\Delta$.

(c) ⇒ (a) By Theorem 5.3.5.2, every non-zero ideal of $\mathcal{O}_\Delta$ is $\mathcal{O}_\Delta$-invertible, and thus it is principal by Theorem 5.5.10. □

According to a classical philosophy of algebraic number theory, the ideal class group $\mathcal{C}_K = \mathcal{C}_{\Delta_K}$ of the maximal order $\mathcal{O}_K$ describes the deviation of $\mathcal{O}_K$ from being factorial. For details and quantitative results supporting this philosophy we refer to [**33**].

Example 5.8.7. Let K be a quadratic number field.

1. If $\Delta_K < 0$, then $\mathcal{O}_K$ is factorial if and only if
$$\Delta_K \in \{-3, -4, -7, -8, -11, -19, -43, -67, -163\}\,.$$
We asserted in Example 1.3.3 that these are the only negative fundamental discriminants Δ satisfying $h_\Delta = 1$. Note however that we did not prove this result (for a proof we refer to [**19**, Theorem 7.30]).
2. If $D \in \{2,\ 3,\ 5,\ 6,\ 7\}$ and $K = \mathbb{Q}(\sqrt{D}\,)$, then $\mathcal{O}_K$ is factorial. Indeed, for the fields in question, we have $\Delta_K \in \{5,\ 8,\ 12,\ 24,\ 28\}$ and $h_K = 1$ by Example 2.2.10. It is conjectured (already since Gauss) that there are infinitely many primes $p \equiv 1 \bmod 4$ such that $h_p = 1$.

Theorem 5.8.8 (Classification of prime ideals)**.** *Let Δ be a quadratic discriminant and p a prime.*

1. *Suppose that* $\mathsf{Q}_\Delta(p) = 1$*, and let $b \in \mathbb{Z}$ be such that* $\Delta \equiv b^2 \bmod 4p$*. Then*
$$\mathfrak{p} = \Big[p, \frac{b+\sqrt{\Delta}}{2}\Big] \quad \textit{and} \quad \mathfrak{p}' = \Big[p, \frac{b-\sqrt{\Delta}}{2}\Big]$$
are the only $\mathcal{O}_\Delta$-regular prime ideals containing p, $p\mathcal{O}_\Delta = \mathfrak{p}\mathfrak{p}'$, $\mathfrak{p} \ne \mathfrak{p}'$, and $\mathfrak{N}_\Delta(\mathfrak{p}) = \mathfrak{N}_\Delta(\mathfrak{p}') = p$.
2. *If $\mathsf{Q}_\Delta(p) = -1$, then $p\,\mathcal{O}_\Delta$ is the only prime ideal of $\mathcal{O}_\Delta$ containing p.*
3. *If $\mathsf{Q}_\Delta(p) = 0$, then there is a unique prime ideal $\mathfrak{p}$ of $\mathcal{O}_\Delta$ containing p.*
   - *If $p \ne 2$, then*
$$\mathfrak{p} = \begin{cases} [p, \sqrt{D}\,] & \textit{if} \quad \Delta = 4D \equiv 0 \bmod 4\,, \\ \Big[p, \dfrac{p+\sqrt{\Delta}}{2}\Big] & \textit{if} \quad \Delta \equiv 1 \bmod 4\,. \end{cases}$$
   - *If $p = 2$, then $\Delta = 4D$, where $D \in \mathbb{Z}$, and*
$$\mathfrak{p} = \begin{cases} [2, \sqrt{D}\,] & \textit{if} \quad 2\,|\,D\,, \\ [2, 1+\sqrt{D}\,] & \textit{if} \quad 2\nmid D\,. \end{cases}$$

   In any case, $\mathfrak{N}_\Delta(\mathfrak{p}) = p$, and $\mathfrak{p}$ has the following properties:
   - *If $p \nmid f_\Delta$, then $\mathfrak{p}$ is $\mathcal{O}_\Delta$-regular and $\mathfrak{p}^2 = p\,\mathcal{O}_\Delta$.*
   - *If $p\,|\,f_\Delta$, then $\mathfrak{p}$ is not $\mathcal{O}_\Delta$-invertible and $\mathfrak{p}^2 = p\,\mathfrak{p}$.*

PROOF. We tacitly apply the Theorems 5.4.2 and 5.8.1.3.

1. If $\mathsf{Q}_\Delta(p) = 1$, then $p \nmid \Delta$ and $\Delta \equiv b^2 \bmod 4p$ for some $b \in \mathbb{Z}$. Hence
$$\Delta \equiv b \bmod 2\,, \quad 4p\,|\,b^2 - \Delta\,, \quad p \nmid b \ \text{ and } \ b \not\equiv -b \bmod 2p\,.$$

$\mathfrak{p}$ and $\mathfrak{p}'$ are $\mathcal{O}_\Delta$-regular prime ideals satisfying $\mathfrak{N}_\Delta(\mathfrak{p}) = \mathfrak{N}_\Delta(\mathfrak{p}') = p$, $\mathfrak{p} \ne \mathfrak{p}'$ and $\mathfrak{p}\mathfrak{p}' = \mathfrak{N}_\Delta(\mathfrak{p})\mathcal{O}_\Delta = p\mathcal{O}_\Delta$. If $\mathfrak{q}$ is any prime ideal of $\mathcal{O}_\Delta$ containing p, then $p\mathcal{O}_\Delta = \mathfrak{p}\mathfrak{p}' \subset \mathfrak{q}$, hence $\mathfrak{p} \subset \mathfrak{q}$ or $\mathfrak{p}' \subset \mathfrak{q}$, and thus $\mathfrak{q} \in \{\mathfrak{p}, \mathfrak{p}'\}$.

2. By Theorem 5.8.4.1, $p\mathcal{O}_\Delta$ is a prime ideal of $\mathcal{O}_\Delta$, and as non-zero prime ideals are maximal, it is the only prime ideal of $\mathcal{O}_\Delta$ containing p.

3. CASE 1: $\Delta = 4D$, where $D \in \mathbb{Z}$ and $p \,|\, D$, say $D = pD'$ for some $D' \in \mathbb{Z}$. Then $\mathfrak{p} = [p, \sqrt{D}\,]$ is an $\mathcal{O}_\Delta$-primitive prime ideal, $\mathfrak{N}_\Delta(\mathfrak{p}) = p \in \mathfrak{p}$, and $\mathfrak{p}$ is $\mathcal{O}_\Delta$-regular if and only if $p \nmid D'$. We calculate

$$\mathfrak{p}^2 = [p^2, p\sqrt{D}\,, D\,] = p\,[p, \sqrt{D}\,, D'] = \begin{cases} p\,\mathfrak{p} & \text{if} \quad p \,|\, D'\,, \\ p\,\mathcal{O}_\Delta & \text{if} \quad p \nmid D'\,, \end{cases}$$

and we assert that $p \,|\, D'$ if and only if $p \,|\, f_\Delta$. Indeed, if $p \,|\, D'$, then $p^2 \,|\, \Delta$ if $p \neq 2$, and $2^4 \,|\, \Delta$ if $p = 2$. In both cases, this implies $p \,|\, f_\Delta$. Thus suppose that $p \nmid D'$. Then we obtain $\mathsf{v}_p(\Delta) = 1$ if $p \neq 2$, and $\mathsf{v}_p(\Delta) = 3$ if $p = 2$. In both cases, this implies $p \nmid f_\Delta$.

CASE 2: $\Delta \equiv 1 \bmod 4$ and $p \,|\, \Delta$, say $\Delta = p\Delta'$. Then

$$\mathfrak{p} = \Big[\,p, \frac{p + \sqrt{\Delta}}{2}\,\Big]$$

is an $\mathcal{O}_\Delta$-primitive prime ideal such that $\mathfrak{N}_\Delta(\mathfrak{p}) = p \in \mathfrak{p}$, and $\mathfrak{p}$ is $\mathcal{O}_\Delta$-regular if and only if $p \nmid \Delta'$, which is equivalent to $p \nmid f_\Delta$. Now we calculate

$$\begin{aligned} \mathfrak{p}^2 &= \Big[p^2, \frac{p^2 + p\sqrt{\Delta}}{2}\,, \frac{p^2 + \Delta + 2p\sqrt{\Delta}}{2}\Big] = \Big[p^2, \frac{p^2 + p\sqrt{\Delta}}{2}, \frac{-p^2 + \Delta}{2}\Big] \\ &= p\,\Big[p, \frac{p + \sqrt{\Delta}}{2}, \frac{-p + \Delta'}{2}\Big] = \begin{cases} p\,\mathfrak{p} & \text{if} \quad p \,|\, \Delta'\,, \\ p\,\mathcal{O}_\Delta & \text{if} \quad p \nmid \Delta'\,. \end{cases} \end{aligned}$$

CASE 3: $p = 2$ and $\Delta = 4D$, where $D \in \mathbb{Z}$ and $2 \nmid D$. Then $\mathfrak{p} = [2, 1 + \sqrt{D}\,]$ is an $\mathcal{O}_\Delta$-primitive prime ideal such that $\mathfrak{N}_\Delta(\mathfrak{p}) = 2 \in \mathfrak{p}$, and $\mathfrak{p}$ is $\mathcal{O}_\Delta$-regular if and only if $(2, 2, (\Delta - 4)/8) = 1$ which is equivalent to $D \equiv 3 \bmod 4$ and thus to $2 \nmid f_\Delta$. Hence we obtain

$$\mathfrak{p}^2 = [4, 2{+}2\sqrt{D},\, 1{+}D{+}2\sqrt{D}\,] = 2\,[2, 1{+}\sqrt{D}, (-1{+}D)/2\,] = \begin{cases} 2\,\mathfrak{p} & \text{if} \quad 2 \,|\, f_\Delta\,, \\ 2\,\mathcal{O}_\Delta & \text{if} \quad 2 \nmid f_\Delta\,. \end{cases} \qquad \Box$$

5.9. Class groups of quadratic orders

In this section we compare the ideal class groups of different orders inside a fixed quadratic number field. The main results are the Mayer-Vietoris sequence in Theorem 5.9.7 and the class number formulas arising from it. Before we can do that, we must investigate the prime residue class groups of quadratic orders and the behavior of extension ideals and contraction ideals. In the second part of the section, we present various applications of the Mayer-Vietoris sequence.

We start with a simple lemma characterizing relative primeness and then we investigate the analogue of Euler's φ function for quadratic orders in Theorem 5.9.3.

Lemma 5.9.1. *Let Δ be a quadratic discriminant and $\mathfrak{a}$ an ideal of $\mathcal{O}_\Delta$.*

1. $(\mathcal{O}_\Delta/\mathfrak{a})^\times = \{\alpha + \mathfrak{a} \mid \alpha \in \mathcal{O}_\Delta\,,\ \mathfrak{a} + \alpha\mathcal{O}_\Delta = \mathcal{O}_\Delta\,\}$. *In particular, if $\gamma \in \mathcal{O}_\Delta$, then* $(\mathcal{O}_\Delta/\gamma\mathcal{O}_\Delta)^\times = \{\alpha + \gamma\mathcal{O}_\Delta \mid \alpha \in \mathcal{O}_\Delta\,,\ (\alpha, \gamma) = 1\,\}$.

2. *If* $\mathfrak{a} \neq \mathbf{0}$ *and* $m \in \mathbb{N}$*, then* $\mathfrak{a} + m\mathcal{O}_\Delta = \mathcal{O}_\Delta$ *if and only if* $(\mathfrak{N}_\Delta(\mathfrak{a}), m) = 1$*, and in this case the map* $\mu_m \colon \mathcal{O}_\Delta/\mathfrak{a} \to \mathcal{O}_\Delta/\mathfrak{a}$*, defined by* $\mu_m(x+\mathfrak{a}) = mx+\mathfrak{a}$ *for all* $x \in \mathcal{O}_\Delta$*, is bijective.*
3. *If* $\mathfrak{p}$ *is a non-zero prime ideal of* $\mathcal{O}_\Delta$ *and* $e \in \mathbb{N}$*, then*

$$(\mathcal{O}_\Delta/\mathfrak{p}^e)^\times = \{\alpha + \mathfrak{p}^e \mid \alpha \in \mathcal{O}_\Delta \setminus \mathfrak{p}\}\,.$$

If $\mathfrak{a}+\alpha\mathcal{O}_\Delta$ for some ideal $\mathfrak{a}$ of $\mathcal{O}_\Delta$ and $\alpha \in \mathcal{O}_\Delta$, then $\mathfrak{a}$ and α are called *coprime.*

Proof. 1. See Lemma A.8.4.

2. If $m \in \mathbb{N}$, then $\mu_m(\mathcal{O}_\Delta/\mathfrak{a}) = \mathfrak{a} + m\mathcal{O}_\Delta/\mathfrak{a} = \mathcal{O}_\Delta/\mathfrak{a}$ holds if and only if $\mathfrak{a} + m\mathcal{O}_\Delta = \mathcal{O}_\Delta$. Since $|\mathcal{O}_\Delta/\mathfrak{a}| = \mathfrak{N}_\Delta(\mathfrak{a}) < \infty$, it follows that $\mathfrak{a} + m\mathcal{O}_\Delta = \mathcal{O}_\Delta$ if and only if μ_m is bijective, that is, if and only if $(\mathfrak{N}_\Delta(\mathfrak{a}), m) = 1$ (see Theorem A.5.8.2).

3. By 1. it suffices to prove: If $\alpha \in \mathcal{O}_\Delta$, then $\mathfrak{p}^e + \alpha\mathcal{O}_\Delta = \mathcal{O}_\Delta$ if and only if $\alpha \notin \mathfrak{p}$. Clearly, $\mathfrak{p}^e + \alpha\mathcal{O}_\Delta = \mathcal{O}_\Delta$ implies $\alpha \notin \mathfrak{p}$. Conversely, if $\mathfrak{p}^e + \alpha\mathcal{O}_\Delta \subsetneq \mathcal{O}_\Delta$, then there exists a prime ideal $\mathfrak{q}$ of $\mathcal{O}_\Delta$ such that $\mathfrak{p}^e + \alpha\mathcal{O}_\Delta \subset \mathfrak{q}$. Since $\mathfrak{p}^e \subset \mathfrak{q}$, we obtain $\mathfrak{p} \subset \mathfrak{q}$, hence $\mathfrak{p} = \mathfrak{q}$, and therefore $\alpha \in \mathfrak{p}$. □

Exercise 5.9.2. Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_\Delta$ and $\alpha \in \mathcal{O}_\Delta$. Prove that $\mathfrak{a}+\alpha\mathcal{O}_\Delta = \mathcal{O}_\Delta$ if and only if $\alpha \notin \mathfrak{p}$ for every prime ideal $\mathfrak{p}$ of $\mathcal{O}_\Delta$ containing $\mathfrak{a}$.

Theorem 5.9.3. *Let* Δ *be a quadratic discriminant and* $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_r^{e_r}$*, where* $r \in \mathbb{N}_0$*,* $e_1, \ldots, e_r \in \mathbb{N}$*, and* $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ *are distinct* $\mathcal{O}_\Delta$*-invertible prime ideals. Then*

$$|(\mathcal{O}_\Delta/\mathfrak{a})^\times| = \prod_{i=1}^r \mathfrak{N}_\Delta(\mathfrak{p}_i)^{e_i-1}(\mathfrak{N}_\Delta(\mathfrak{p}_i) - 1) = \mathfrak{N}_\Delta(\mathfrak{a}) \prod_{i=1}^r \Big(1 - \frac{1}{\mathfrak{N}_\Delta(\mathfrak{p}_i)}\Big)\,.$$

Proof. We use throughout that $\mathfrak{N}_\Delta$ is multiplicative on the set of invertible ideals (see Theorem 5.4.6).

CASE 1: $r = 1$. Suppose that $\mathfrak{a} = \mathfrak{p}^e$, where $\mathfrak{p}$ is an $\mathcal{O}_\Delta$-invertible prime ideal and $e \in \mathbb{N}$. We proceed by induction on e.

$e = 1$: $\mathcal{O}_\Delta/\mathfrak{p}$ is a field, and $|(\mathcal{O}_\Delta/\mathfrak{p})^\times| = |\mathcal{O}_\Delta/\mathfrak{p}| - 1 = \mathfrak{N}_\Delta(\mathfrak{p}) - 1$.

$e \geq 2$, $e-1 \to e$: It suffices to construct an exact sequence

$$\mathbf{0} \;\to\; \mathcal{O}_\Delta/\mathfrak{p} \;\overset{\vartheta}{\to}\; (\mathcal{O}_\Delta/\mathfrak{p}^e)^\times \;\overset{\theta}{\to}\; (\mathcal{O}_\Delta/\mathfrak{p}^{e-1})^\times \;\to\; \mathbf{1}\,,$$

for then it follows by the induction hypothesis that

$$\begin{aligned}|(\mathcal{O}_\Delta/\mathfrak{p}^e)^\times| &= |(\mathcal{O}_\Delta/\mathfrak{p}^{e-1})^\times|\,|\mathcal{O}_\Delta/\mathfrak{p}| = \mathfrak{N}_\Delta(\mathfrak{p}^{e-2})(\mathfrak{N}_\Delta(\mathfrak{p}) - 1)\mathfrak{N}_\Delta(\mathfrak{p}) \\ &= \mathfrak{N}(\mathfrak{p})^{e-1}(\mathfrak{N}(\mathfrak{p}) - 1)\,.\end{aligned}$$

Observe that $(\mathcal{O}_\Delta/\mathfrak{p}^e)^\times = \{\alpha + \mathfrak{p}^e \mid \alpha \in \mathcal{O}_\Delta \setminus \mathfrak{p}\}$. Hence there is an epimorphism $\theta \colon (\mathcal{O}_\Delta/\mathfrak{p}^e)^\times \to (\mathcal{O}_\Delta/\mathfrak{p}^{e-1})^\times$ such that $\theta(\alpha + \mathfrak{p}^e) = \alpha + \mathfrak{p}^{e-1}$ for all $\alpha \in \mathcal{O}_\Delta \setminus \mathfrak{p}$, and $\mathrm{Ker}(\theta) = \{b + \mathfrak{p}^e \mid b \in 1 + \mathfrak{p}^{e-1}\}$. We fix some element $c \in \mathfrak{p}^{e-1} \setminus \mathfrak{p}^e$, and we define $\vartheta \colon \mathcal{O}_\Delta/\mathfrak{p} \to (\mathcal{O}_\Delta/\mathfrak{p}^e)^\times$ by $\vartheta(a + \mathfrak{p}) = 1 + ca + \mathfrak{p}^e$. If $a, a' \in \mathcal{O}_\Delta$ and $a \equiv a' \bmod \mathfrak{p}$, then $1 + ca \equiv 1 + ca' \bmod \mathfrak{p}^e$, and since $cc' \in \mathfrak{p}^{2e-2} \subset \mathfrak{p}^e$, we get $1 + c(a + a') \equiv (1 + ca)(1 + ca') \bmod \mathfrak{p}^e$. Hence ϑ is a group homomorphism, and obviously $\mathrm{Im}(\vartheta) \subset \mathrm{Ker}(\theta)$.

To prove the reverse inclusion, we note first that $\mathfrak{p}^{e-1} = \mathfrak{p}^e + c\mathcal{O}_\Delta$. Indeed, obviously $\mathfrak{p}^{e-1} \supset \mathfrak{p}^e + c\mathcal{O}_\Delta$, and since $\mathfrak{p}^{e-1}$ is $\mathcal{O}_\Delta$-invertible, there exists some ideal $\mathfrak{c}$ of $\mathcal{O}_\Delta$ such that $\mathfrak{p}^e \subsetneq \mathfrak{p}^e + c\mathcal{O}_\Delta = \mathfrak{p}^{e-1}\mathfrak{c}$, hence $\mathfrak{p} \subsetneq \mathfrak{c}$, and therefore $\mathfrak{c} = \mathcal{O}_\Delta$ and $\mathfrak{p}^{e-1} = \mathfrak{p}^e + c\mathcal{O}_\Delta$. Assume now that $b + \mathfrak{p}^e \in \operatorname{Ker}(\theta)$, where $b \in 1 + \mathfrak{p}^{e-1} = 1 + \mathfrak{p}^e + c\mathcal{O}_\Delta$. Then there exists some $a \in \mathcal{O}_\Delta$ such that $b + \mathfrak{p}^e = 1 + ca + \mathfrak{p}^e = \vartheta(a + \mathfrak{p})$.

CASE 2 : $r \ge 2$. By the Chinese remainder theorem there exists a group isomorphism $(\mathcal{O}_\Delta/\mathfrak{a})^\times \overset{\sim}{\to} (\mathcal{O}_\Delta/\mathfrak{p}_1^{e_1})^\times \times \ldots \times (\mathcal{O}_\Delta/\mathfrak{p}_r^{e_r})^\times$, and we obtain

$$\begin{aligned} |(\mathcal{O}_\Delta/\mathfrak{a})^\times| &= \prod_{i=1}^r |(\mathcal{O}_\Delta/\mathfrak{p}_i^{e_i})^\times| = \prod_{i=1}^r \mathfrak{N}_\Delta(\mathfrak{p}_i)^{e_i-1}(\mathfrak{N}_\Delta(\mathfrak{p}_i) - 1) \\ &= \prod_{i=1}^r \mathfrak{N}_\Delta(\mathfrak{p}_i^{e_i} \prod_{i=1}^r \Big(1 - \frac{1}{\mathfrak{N}_\Delta(\mathfrak{p}_i)}\Big) = \mathfrak{N}_\Delta(\mathfrak{a}) \prod_{i=1}^r \Big(1 - \frac{1}{\mathfrak{N}_\Delta(\mathfrak{p}_i)}\Big). \qquad \square \end{aligned}$$

We can supplement Theorem 5.9.3 by a calculation of $(\mathcal{O}_\Delta/m\mathcal{O}_\Delta)^\times$ for positive integers m, even if they are not coprime to the conductor.

Theorem 5.9.4. *Let Δ be a quadratic discriminant and $m \in \mathbb{N}$. Then*

$$|(\mathcal{O}_\Delta/m\mathcal{O}_\Delta)^\times| = m^2 \prod_{p\,|\,m} \Big(1 - \frac{1}{p}\Big)\Big(1 - \frac{\mathsf{Q}_\Delta(p)}{p}\Big).$$

PROOF. If $m = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$, where $r \in \mathbb{N}$, $e_1, \ldots, e_r \in \mathbb{N}$ and $p_1, \ldots, p_r$ are distinct primes, then the Chinese remainder theorem yields a group isomorphism $(\mathcal{O}_\Delta/m\mathcal{O}_\Delta)^\times \overset{\sim}{\to} (\mathcal{O}_\Delta/p_1^{e_1}\mathcal{O}_\Delta)^\times \times \ldots \times (\mathcal{O}_\Delta/p_r^{e_r}\mathcal{O}_\Delta)^\times$, and therefore it suffices to prove that

$$|(\mathcal{O}_\Delta)/p^e\mathcal{O}_\Delta)^\times| = p^{2e}\Big(1 - \frac{1}{p}\Big)\Big(1 - \frac{\mathsf{Q}_\Delta(p)}{p}\Big) \quad \text{for all primes } p \text{ and } e \ge 1.$$

If p is a prime not dividing the conductor f_Δ of Δ, this follows by Theorem 5.9.3.

Assume now that p is a prime such that $\mathsf{v}_p(f_\Delta) = n \ge 1$ and $e \in \mathbb{N}$. Then $\Delta = \Delta_1 p^{2n}$ for some quadratic discriminant Δ_1, and $p \nmid f_{\Delta_1}$. We set $\Delta_1 = 4D_1 + \sigma_1$, where $D_1 \in \mathbb{Z}$, $\sigma_1 \in \{0, 1\}$, and we denote by $\omega_1 = \omega_{\Delta_1}$ the basis number of discriminant Δ_1. Then it follows that $\mathcal{O}_\Delta = \mathbb{Z} + p^n\omega_1\mathbb{Z}$, $p^e\mathcal{O}_\Delta \cap \mathbb{Z} = p^e\mathbb{Z}$, and the inclusion $\mathbb{Z} \hookrightarrow \mathcal{O}_\Delta$ induces a ring monomorphism $j\colon \mathbb{Z}/p^e\mathbb{Z} \to \mathcal{O}_\Delta/p^e\mathcal{O}_\Delta$, given by $j(a + p^e\mathbb{Z}) = a + p^e\mathcal{O}_\Delta$ for all $a \in \mathbb{Z}$. We set $A = j(\mathbb{Z}/p^e\mathbb{Z})$ and obtain $\mathcal{O}_\Delta/p^e\mathcal{O}_\Delta = A[\eta]$, where $\eta = p^n\omega_1 + p^e\mathcal{O}_\Delta$. Since $\omega_1^2 = \sigma_1\omega_1 + p^{2n}D_1$, it follows that $\eta^2 = \sigma_1 p^n \eta + p^{2n}\overline{D}_1$, where $\overline{D}_1 = D_1 + p^e\mathcal{O}_\Delta$. Hence it suffices to prove the following assertion.

A. Every $\xi \in \mathcal{O}_\Delta/p^e\mathcal{O}_\Delta$ has a unique representation $\xi = \alpha + \beta\eta$ for some $\alpha, \beta \in A$, and then we have $\xi \in (\mathcal{O}_\Delta/p^e\mathcal{O}_\Delta)^\times$ if and only if $\alpha \in A^\times$.

Indeed, by **A** we easily get

$$|(\mathcal{O}_\Delta/p^e\mathcal{O}_\Delta)^\times| = |A|\,|A^\times| = |\mathbb{Z}/p^e\mathbb{Z}|\,|(\mathbb{Z}/p^e\mathbb{Z})^\times| = p^e\,[p^{e-1}(p-1)] = p^{2e-1}(p-1).$$

Proof of **A.** Since $\mathcal{O}_\Delta/p^e\mathcal{O}_\Delta = A[\eta]$ and $\eta^2 = \sigma_1 p^n\eta + p^{2n}\overline{D}_1$, it follows that every $\xi \in \mathcal{O}_\Delta/p^e\mathcal{O}_\Delta$ has a representation as asserted. As to uniqueness, it suffices to prove that, for all $\alpha, \beta \in A$, $\alpha + \beta\eta = 0$ implies $\alpha = \beta = 0$. Thus suppose that

$\alpha = a + p^e\mathcal{O}_\Delta,\ \beta = b + p^e\mathcal{O}_\Delta \in A$, where $a,\ b \in \mathbb{Z}$, and $\alpha + \beta\eta = 0$. Then there exist $u,\ v \in \mathbb{Z}$ such that $a + bp^n\omega_1 = p^e(u + p^n\omega_1 v)$, which implies that $a = p^e u,\ \ b = p^e v$, and therefore $\alpha = \beta = 0$.

Assume now that $\alpha = a + p^e\mathcal{O}_\Delta,\ \beta = b + p^e\mathcal{O}_\Delta \in A$ (where $a,\ b \in \mathbb{Z}$) and $\alpha + \beta\eta \in (\mathcal{O}/p^e\mathcal{O})^\times$. Then there exist $\alpha_1 = a_1 + p^e\mathcal{O}_\Delta,\ \beta_1 = b_1 + p^e\mathcal{O}_\Delta \in A$ (where $a_1,\ b_1 \in \mathbb{Z}$) such that

$$(\alpha + \beta\eta)(\alpha_1 + \beta\eta) = \alpha\alpha_1 + (\alpha\beta_1 + \alpha_1\beta)\eta + \beta\beta_1(\sigma_1 p^n + p^{2n}\overline{D}_1) = 1 \in \mathcal{O}_\Delta/p^e\mathcal{O}_\Delta\,.$$

It follows that $1 = \alpha\alpha_1 + p^{2n}\beta\beta_1\overline{D}_1 = aa_1 + p^{2n}bb_1D_1 + p^e\mathbb{Z}$, hence $aa_1 \equiv 1 \mod p$, $a + p^e\mathbb{Z} \in (\mathbb{Z}/p^e\mathbb{Z})^\times$ and $\alpha \in A^\times$.

Conversely, assume that $\alpha \in A^\times,\ \ \beta \in A$ and $\xi = \alpha + \beta\eta = \alpha(1 - \eta_1)$, where $\eta_1 = -\alpha^{-1}\beta\eta$. Since $(p^n\omega_1)^e \in p^e\mathcal{O}_\Delta$, it follows that $\eta_1^e = 0$ and

$$(1 - \eta_1)(1 + \eta_1 + \ldots + \eta_1^{e-1}) = 1 - \eta_1^e = 1\,.$$

Hence we obtain $1 - \eta_1 \in (\mathcal{O}_\Delta/p^e\mathcal{O}_\Delta)^\times$, and therefore also $\xi \in (\mathcal{O}_\Delta/p^e\mathcal{O}_\Delta)^\times$. □

Let Δ be a quadratic discriminant and $d \in \mathbb{N}$. We want to compare the ideals (and then also the ideal class groups and narrow ideal class groups) of the orders $\mathcal{O}_\Delta$ and $\mathcal{O}_{\Delta d^2}$. For this, we introduce the following notations.

For a quadratic discriminant Δ and $\alpha \in \mathcal{O}_\Delta$, we denote by

- $\mathcal{I}_\Delta^{(\alpha)}$ the set of all non-zero ideals $\mathfrak{a}$ of $\mathcal{O}_\Delta$ which are coprime to α [that means, $\mathfrak{a} + \alpha\mathcal{O}_\Delta = \mathcal{O}_\Delta$], and by
- $\mathcal{I}_\Delta = \mathcal{I}_\Delta^{(1)}$ the set of all non-zero ideals of $\mathcal{O}_\Delta$.

If $\mathfrak{a},\ \mathfrak{b} \in \mathcal{I}_\Delta^{(\alpha)}$, then $\mathcal{O}_\Delta = (\mathfrak{a} + \alpha\mathcal{O}_\Delta)(\mathfrak{b} + \alpha\mathcal{O}_\Delta) \subset \mathfrak{ab} + \alpha\mathcal{O}_\Delta \subset \mathcal{O}_\Delta$, and therefore $\mathfrak{ab} + \alpha\mathcal{O}_\Delta = \mathcal{O}_\Delta$, whence $\mathfrak{ab} \in \mathcal{I}_\Delta^{(\alpha)}$. Hence $\mathcal{I}_\Delta^{(\alpha)}$ is a submonoid of $\mathcal{I}_\Delta$.

If $m \in \mathbb{N}$, then Lemma 5.9.1 implies that a non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_\Delta$ belongs to $\mathcal{I}_\Delta^{(m)}$ if and only if $(\mathfrak{N}_\Delta(\mathfrak{a}), m) = 1$. In particular, if $f_\Delta \,|\, m$, then all ideals $\mathfrak{a} \in \mathcal{I}_\Delta^{(m)}$ satisfy $(\mathfrak{N}_\Delta(\mathfrak{a}), f_\Delta) = 1$, and thus they are $\mathcal{O}_\Delta$-invertible (see Corollary 5.4.3).

For $d \in \mathbb{N}$ and an ideal $\mathfrak{a}$ of $\mathcal{O}_{\Delta d^2}$, we denote by $\mathfrak{a}\mathcal{O}_\Delta$ the ideal of $\mathcal{O}_\Delta$ generated by $\mathfrak{a}$.

Theorem 5.9.5. *Let Δ be a quadratic discriminant and $d \in \mathbb{N}$.*

1. *If $m \in \mathbb{N}$ and $d \,|\, m$, then the maps*

$$\Phi\colon \mathcal{I}_\Delta^{(m)} \to \mathcal{I}_{\Delta d^2}^{(m)}\,, \quad \textit{defined by} \quad \Phi(\mathfrak{A}) = \mathfrak{A} \cap \mathcal{O}_{\Delta d^2} \quad \textit{for all } \ \mathfrak{A} \in \mathcal{I}_\Delta^{(m)}\,,$$

and

$$\Phi_1\colon \mathcal{I}_{\Delta d^2}^{(m)} \to \mathcal{I}_\Delta^{(m)}\,, \quad \textit{defined by} \quad \Phi_1(\mathfrak{a}) = \mathfrak{a}\mathcal{O}_\Delta \quad \textit{for all } \ \mathfrak{a} \in \mathcal{I}_{\Delta d^2}^{(m)}\,,$$

are mutually inverse monoid isomorphisms, and

$$\mathfrak{N}_\Delta(\mathfrak{A}) = \mathfrak{N}_{\Delta d^2}(\mathfrak{A} \cap \mathcal{O}_{\Delta d^2}) \quad \textit{for all } \ \mathfrak{A} \in \mathcal{I}_\Delta^{(m)}.$$

2. *Suppose that* $\mathfrak{a} \in \mathcal{J}_{\Delta d^2}^{(d)}$*, and let* $e \in \mathbb{N}$ *be such that* $e^{-1}\mathfrak{a}$ *is* $\mathcal{O}_{\Delta d^2}$*-primitive. Then there exists some* $b \in \mathbb{Z}$ *such that*

$$b \equiv \Delta \bmod 2 \quad \textit{and} \quad \mathfrak{a} = e\Big[\,a,\ \frac{bd+\sqrt{\Delta d^2}}{2}\,\Big],$$

and for each such b *we obtain*

$$\mathfrak{a}\mathcal{O}_\Delta = e\Big[\,a,\ \frac{b+\sqrt{\Delta}}{2}\,\Big].$$

Moreover, $\mathfrak{a}$ *is* $\mathcal{O}_{\Delta d^2}$*-primitive* [$\mathcal{O}_{\Delta d^2}$*-invertible,* $\mathcal{O}_{\Delta d^2}$*-regular*] *if and only if* $\mathfrak{a}\mathcal{O}_\Delta$ *is* $\mathcal{O}_\Delta$*-primitive* [$\mathcal{O}_{\Delta d^2}$*-invertible,* $\mathcal{O}_{\Delta d^2}$*-regular*]*.*

PROOF. 1. If $\mathfrak{A} \in \mathcal{J}_\Delta^{(m)}$, then $\mathfrak{A} \cap \mathcal{O}_{\Delta d^2}$ is a non-zero ideal of $\mathcal{O}_{\Delta d^2}$, and the inclusion $\mathcal{O}_{\Delta d^2} \hookrightarrow \mathcal{O}_\Delta$ induces a monomorphism $\mathcal{O}_{\Delta d^2}/\mathfrak{A} \cap \mathcal{O}_{\Delta d^2} \to \mathcal{O}_\Delta/\mathfrak{A}$. It follows that $\mathfrak{N}_{\Delta d^2}(\mathfrak{A} \cap \mathcal{O}_{\Delta d^2}) \,|\, \mathfrak{N}_\Delta(\mathfrak{A})$, hence $(\mathfrak{N}_{\Delta d^2}(\mathfrak{A} \cap \mathcal{O}_{\Delta d^2}), m) = 1$, and therefore $\mathfrak{A} \cap \mathcal{O}_{\Delta d^2} \in \mathcal{J}_{\Delta d^2}^{(m)}$. By Lemma 5.9.1, and since $m\mathcal{O}_\Delta \subset d\mathcal{O}_\Delta \subset \mathcal{O}_{\Delta d^2}$, we obtain $\mathcal{O}_\Delta/\mathfrak{A} = m(\mathcal{O}_\Delta/\mathfrak{A}) = (m\mathcal{O}_\Delta + \mathfrak{A})/\mathfrak{A} \subset (\mathcal{O}_{\Delta d^2} + \mathfrak{A})/\mathfrak{A} \cong \mathcal{O}_{\Delta d^2}/\mathcal{O}_{\Delta d^2} \cap \mathfrak{A}$. But this implies that $\mathfrak{N}_\Delta(\mathfrak{A}) \le \mathfrak{N}_{\Delta d^2}(\mathcal{O}_{\Delta d^2} \cap \mathfrak{A})$, and therefore equality holds.

So far we have proved that $\Phi\colon \mathcal{J}_\Delta^{(m)} \to \mathcal{J}_{\Delta d^2}^{(m)}$, defined by $\Phi(\mathfrak{A}) = \mathfrak{A} \cap \mathcal{O}_{\Delta d^2}$, is a map satisfying $\mathfrak{N}_{\Delta d^2}(\mathfrak{A} \cap \mathcal{O}_{\Delta d^2}) = \mathfrak{N}_\Delta(\mathfrak{A})$ for all $\mathfrak{A} \in \mathcal{J}_\Delta^{(m)}$. To complete the proof of 1., it suffices to show the following two assertions:

A. If $\mathfrak{a} \in \mathcal{J}_{\Delta d^2}^{(m)}$, then $\mathfrak{a}\mathcal{O}_\Delta \in \mathcal{J}_\Delta^{(m)}$, and $\mathfrak{a}\mathcal{O}_\Delta \cap \mathcal{O}_{\Delta d^2} = \mathfrak{a}$.

B. If $\mathfrak{A} \in \mathcal{J}_\Delta^{(m)}$, then $(\mathfrak{A} \cap \mathcal{O}_{\Delta d^2})\mathcal{O}_\Delta = \mathfrak{A}$.

Indeed, **A** and **B** imply that Φ is bijective, and $\Phi^{-1}(\mathfrak{a}) = \mathfrak{a}\mathcal{O}_\Delta = \Phi_1(\mathfrak{a})$ for all $\mathfrak{a} \in \mathcal{J}_{\Delta d^2}^{(m)}$. Since $(\mathfrak{a}\mathfrak{b})\mathcal{O}_\Delta = (\mathfrak{a}\mathcal{O}_\Delta)(\mathfrak{b}\mathcal{O}_\Delta)$ for all $\mathfrak{a}, \mathfrak{b} \in \mathcal{J}_{\Delta d^2}^{(m)}$, it follows that Φ_1 is a homomorphism. Hence Φ and Φ_1 are mutually inverse isomorphisms.

Proof of **A.** If $\mathfrak{a} \in \mathcal{J}_{\Delta d^2}^{(m)}$, then $\mathcal{O}_\Delta = (\mathfrak{a} + m\mathcal{O}_{\Delta d^2})\mathcal{O}_\Delta = \mathfrak{a}\mathcal{O}_\Delta + m\mathcal{O}_\Delta$, and therefore $\mathfrak{a}\mathcal{O}_\Delta \in \mathcal{J}_\Delta^{(m)}$. Obviously, $\mathfrak{a} \subset \mathfrak{a}\mathcal{O}_\Delta \cap \mathcal{O}_{\Delta d^2}$, and since

$$\begin{aligned}\mathfrak{a}\mathcal{O}_\Delta \cap \mathcal{O}_{\Delta d^2} &= (\mathfrak{a}\mathcal{O}_\Delta \cap \mathcal{O}_{\Delta d^2})(\mathfrak{a} + m\mathcal{O}_{\Delta d^2}) \subset \mathfrak{a} + m(\mathfrak{a}\mathcal{O}_\Delta \cap \mathcal{O}_{\Delta d^2})\\ &\subset \mathfrak{a} + \mathfrak{a}m\mathcal{O}_\Delta \subset \mathfrak{a} + \mathfrak{a}\mathcal{O}_{\Delta d^2} = \mathfrak{a}\,,\end{aligned}$$

it follows that $\mathfrak{a} = \mathfrak{a}\mathcal{O}_\Delta \cap \mathcal{O}_{\Delta d^2}$.

Proof of **B.** If $\mathfrak{A} \in \mathcal{J}_\Delta^{(m)}$, then $(\mathfrak{A} \cap \mathcal{O}_{\Delta d^2})\mathcal{O}_\Delta \subset \mathfrak{A}$. On the other hand, since $m\mathfrak{A} \subset \mathfrak{A} \cap m\mathcal{O}_\Delta \subset (\mathfrak{A} \cap \mathcal{O}_{\Delta d^2})\mathcal{O}_\Delta$ and $\mathfrak{A} \cap \mathcal{O}_{\Delta d^2} \in \mathcal{J}_{\Delta d^2}^{(m)}$, we obtain

$$\mathfrak{A} = \mathfrak{A}\mathcal{O}_{\Delta d^2} = \mathfrak{A}(\mathfrak{A} \cap \mathcal{O}_{\Delta d^2} + m\mathcal{O}_{\Delta d^2}) \subset (\mathfrak{A} \cap \mathcal{O}_{\Delta d^2})\mathcal{O}_\Delta + m\mathfrak{A} = (\mathfrak{A} \cap \mathcal{O}_{\Delta d^2})\mathcal{O}_\Delta\,,$$

and therefore $(\mathfrak{A} \cap \mathcal{O}_{\Delta d^2})\mathcal{O}_\Delta = \mathfrak{A}$.

2. If $a = \mathfrak{N}_{\Delta d^2}(e^{-1}\mathfrak{a})$, then $ae^2 = \mathfrak{N}_{\Delta d^2}(\mathfrak{a})$, hence $(a, d) = 1$, and by Theorem 5.4.2 there exists some $b_1 \in \mathbb{Z}$ such that $b_1 \equiv \Delta d^2 \equiv \Delta d \bmod 2$, and

$$\mathfrak{a} = e\Big[\,a,\ \frac{b_1+\sqrt{\Delta d^2}}{2}\,\Big].$$

Let $u,\,l \in \mathbb{Z}$ be such that $b_1 = \Delta d + 2u$ and $al \equiv -u \bmod d$, say $al = -u + kd$ for some $k \in \mathbb{Z}$. If $b = \Delta + 2k$, then $b \equiv \Delta \bmod 2$, $bd = b_1 + 2al$, and therefore

$$\mathfrak{a} = e\left[a, \frac{bd + \sqrt{\Delta d^2}}{2}\right].$$

Assume now that b is chosen in this way. Then it follows that

$$\mathfrak{a} = ea\,[1, d\xi], \quad \text{where} \quad \xi = \frac{b + \sqrt{\Delta}}{2a},$$

$b \equiv \Delta \bmod 2$ implies $\mathcal{O}_\Delta = [1, a\xi]$, and since $(a,d) = 1$, we obtain

$$\mathfrak{a}\mathcal{O}_\Delta = ea\,[1, d\xi]\,[1, a\xi] = ea\,[1, d\xi, a\xi, ad\xi^2] = ea\,[1, \xi] = e\left[a, \frac{b + \sqrt{\Delta}}{2}\right].$$

By definition, we have $e = 1$ if and only if $\mathfrak{a}$ is $\mathcal{O}_{\Delta d^2}$-primitive, and also if and only if $\mathfrak{a}\mathcal{O}_\Delta$ is $\mathcal{O}_\Delta$-primitive.

Let $c_1 \in \mathbb{Z}$ be such that $\Delta d^2 = b^2 d^2 - 4ac_1$. Since $b \equiv \Delta \bmod 2$, it follows that $b^2 \equiv \Delta \bmod 4$, and as $(a,d) = 1$,

$$\frac{b^2 - \Delta}{4}\,d^2 = ac_1 \quad \text{implies} \quad d^2 \mid c_1\,, \quad \text{say} \quad c_1 = d^2 c\,.$$

Then $\Delta = b^2 - 4ac$, and $(a, b, c) = (a, bd, cd^2)$. By Theorem 5.4.2, $\mathfrak{a}$ is $\mathcal{O}_{\Delta d^2}$-invertible if and only if $\mathfrak{a}\mathcal{O}_\Delta$ is $\mathcal{O}_\Delta$-invertible. □

Exercise 5.9.6. Let Δ be a quadratic discriminant, $K = \mathbb{Q}(\sqrt{\Delta}\,)$, $d \in \mathbb{N}$ and $\mathfrak{a}$ a fractional $\mathcal{O}_{\Delta d^2}$-ideal. Prove the following assertions:

a) $\mathfrak{a}\mathcal{O}_\Delta$ is a fractional $\mathcal{O}_\Delta$-ideal. If $\mathfrak{a}$ is $\mathcal{O}_{\Delta d^2}$-invertible, then $\mathfrak{a}\mathcal{O}_\Delta$ is $\mathcal{O}_\Delta$-invertible, and $(\mathcal{O}_\Delta :_K \mathfrak{a}\mathcal{O}_\Delta) = (\mathcal{O}_{\Delta d^2} :_K \mathfrak{a})\mathcal{O}_\Delta$.

b) Let $\mathfrak{b}$ be a lattice in $\mathbb{Q}(\sqrt{\Delta}\,)$. Then

$$(\mathfrak{a}\mathcal{O}_\Delta :_K \mathfrak{b}) = (\mathfrak{a}\mathcal{O}_\Delta :_K \mathfrak{b}\mathcal{O}_\Delta) \supset (\mathfrak{a} :_K \mathfrak{b})\mathcal{O}_\Delta\,,$$

and equality holds if $(\mathfrak{N}_{\Delta d^2}(\mathfrak{a}), d) = 1$.

Theorem 5.9.7. *Let Δ be a quadratic discriminant and $d \in \mathbb{N}$.*

1. *There is a surjective group homomorphism*

$$\Psi^{(+)} = \Psi^{(+)}_{\Delta,d} \colon \mathcal{C}^{(+)}_{\Delta d^2} \;\to\; \mathcal{C}^{(+)}_{\Delta}$$

such that $\Psi^{(+)}([\mathfrak{a}]^{(+)}) = [\mathfrak{a}\mathcal{O}_\Delta]^{(+)}$ for every $\mathcal{O}_{\Delta d^2}$-regular ideal $\mathfrak{a} \in \mathcal{J}^{(d)}_{\Delta d^2}$.

2. *There is a group homomorphism*

$$\vartheta^{(+)} = \vartheta^{(+)}_{\Delta,d} \colon (\mathcal{O}_\Delta/d\mathcal{O}_\Delta)^\times \;\to\; \mathcal{C}^{(+)}_{\Delta d^2}$$

such that $\vartheta^{(+)}(\alpha + d\mathcal{O}_\Delta) = [\alpha\mathcal{O}_\Delta \cap \mathcal{O}_{\Delta d^2}]^{(+)}$ for all $\alpha \in \mathcal{O}_\Delta$ satisfying $(\alpha, d) = 1$ (and $\mathcal{N}(\alpha) > 0$), and

$$|\mathrm{Ker}(\vartheta^{(+)})| = \varphi(d)\,(\mathcal{O}_\Delta^{\times(+)} : \mathcal{O}_{\Delta d^2}^{\times(+)})\,,$$

where $\varphi(d) = |(\mathbb{Z}/d\mathbb{Z})^\times|$, and $(\mathcal{O}_\Delta^{\times(+)} : \mathcal{O}_{\Delta d^2}^{\times(+)})$ denotes the index of the (norm-positive) unit groups.

3. *The homomorphisms* $\Psi^{(+)}$ *and* $\vartheta^{(+)}$ *induce an exact sequence* (called the Mayer-Vietoris sequence)

$$\mathbf{1} \;\to\; \mathrm{Ker}(\vartheta^{(+)}) \;\hookrightarrow\; (\mathcal{O}_\Delta/d\mathcal{O}_\Delta)^\times \;\overset{\vartheta^{(+)}}{\to}\; \mathcal{C}^{(+)}_{\Delta d^2} \;\overset{\Psi^{(+)}}{\to}\; \mathcal{C}^{(+)}_{\Delta} \;\to\; \mathbf{1}\,,$$

and the class number formula

$$h^{(+)}_{\Delta d^2} = h^{(+)}_{\Delta}\,\frac{d}{(\mathcal{O}^{\times(+)}_{\Delta}\,{:}\,\mathcal{O}^{\times(+)}_{\Delta d^2})}\prod_{p\,|\,d}\Bigl(1-\frac{\mathsf{Q}_\Delta(p)}{p}\Bigr)\,.$$

Proof. We tacitly apply the Theorems 5.9.5 and 5.5.7.2(b).

1. If $\mathfrak{a}\in\mathcal{J}^{(d)}_{\Delta d^2}$ is $\mathcal{O}_{\Delta d^2}$-regular, then $\mathfrak{a}\mathcal{O}_\Delta$ is $\mathcal{O}_\Delta$-regular, and $(\lambda\mathfrak{a})\mathcal{O}_\Delta=\lambda(\mathfrak{a}\mathcal{O}_\Delta)$ for all $\lambda\in K^\times$. Every class in $\mathcal{C}^{(+)}_{\Delta d^2}$ contains an $\mathcal{O}_{\Delta d^2}$-regular ideal $\mathfrak{a}\in\mathcal{J}^{(d)}_{\Delta d^2}$, and therefore the assignment $\mathfrak{a}\mapsto\mathfrak{a}\mathcal{O}_\Delta$ defines a map $\Psi^{(+)}\colon\mathcal{C}^{(+)}_{\Delta d^2}\to\mathcal{C}^{(+)}_{\Delta}$ such that $\Psi^{(+)}([\mathfrak{a}]^{(+)})=[\mathfrak{a}\mathcal{O}_\Delta]^{(+)}$ for all $\mathcal{O}_{\Delta d^2}$-regular ideals $\mathfrak{a}\in\mathcal{J}^{(d)}_{\Delta d^2}$. Moreover, since $\mathfrak{a}\mathfrak{b}\mathcal{O}_\Delta=(\mathfrak{a}\mathcal{O}_\Delta)(\mathfrak{b}\mathcal{O}_\Delta)$ for all ideals $\mathfrak{a}$, $\mathfrak{b}$ of $\mathcal{O}_{\Delta d^2}$, it follows that $\Psi^{(+)}$ is a group homomorphism. It remains to prove that $\Psi^{(+)}$ is surjective.

Let $C\in\mathcal{C}^{(+)}_{\Delta}$ be a (narrow) regular ideal class and $\mathfrak{A}\in\mathcal{J}^{(d)}_{\Delta}\cap C$ an $\mathcal{O}_\Delta$-regular ideal. Since $\mathfrak{A}\cap\mathcal{O}_{\Delta d^2}\in\mathcal{J}^{(d)}_{\Delta d^2}$ is an $\mathcal{O}_{\Delta d^2}$-regular ideal and $\mathfrak{A}=(\mathfrak{A}\cap\mathcal{O}_{\Delta d^2})\mathcal{O}_\Delta$, it follows that $C=\Psi([\mathfrak{A}\cap\mathcal{O}_{\Delta d^2}]^{(+)})$.

2. We prove first:

A. If $\alpha,\,\alpha_1\in\mathcal{O}_\Delta$ are such that $(\alpha,d)=1$, $(\alpha_1,d)=1$ (and $\mathcal{N}(\alpha)>0$, $\mathcal{N}(\alpha_1)>0$), then

- $\alpha\alpha_1\mathcal{O}_\Delta\cap\mathcal{O}_{\Delta d^2}=(\alpha\mathcal{O}_\Delta\cap\mathcal{O}_{\Delta d^2})(\alpha_1\mathcal{O}_\Delta\cap\mathcal{O}_{\Delta d^2})$, and
- $\alpha\equiv\alpha_1 \bmod d\mathcal{O}_\Delta$ implies $[\alpha\mathcal{O}_\Delta\cap\mathcal{O}_{\Delta d^2}]^{(+)}=[\alpha_1\mathcal{O}_\Delta\cap\mathcal{O}_{\Delta d^2}]^{(+)}$.

Proof of **A.** The first assertion follows since the map Φ in Theorem 5.9.5 is a homomorphism. Assume now that $\alpha\equiv\alpha_1 \bmod d\mathcal{O}_\Delta$, and let $\beta\in\mathcal{O}_\Delta$ be such that $\alpha\beta\equiv1 \bmod d\mathcal{O}_\Delta$ (and $\mathcal{N}(\beta)>0$). Then we obtain $\alpha\beta\in\mathcal{O}_{\Delta d^2}$, and therefore $\alpha\beta\mathcal{O}_{\Delta d^2}=\alpha\beta\mathcal{O}_\Delta\cap\mathcal{O}_{\Delta d^2}=(\alpha\mathcal{O}_\Delta\cap\mathcal{O}_{\Delta d^2})(\beta\mathcal{O}_\Delta\cap\mathcal{O}_{\Delta d^2})$ (and $\mathcal{N}(\alpha\beta)>0$). This implies

$$[\mathcal{O}_{\Delta d^2}]^{(+)}=[\alpha\mathcal{O}_\Delta\cap\mathcal{O}_{\Delta d^2}]^{(+)}\,[\beta\mathcal{O}_\Delta\cap\mathcal{O}_{\Delta d^2}]^{(+)}\,.$$

In the same way, $\alpha_1\beta\equiv1 \bmod d\mathcal{O}_\Delta$ implies

$$[\mathcal{O}_{\Delta d^2}]^{(+)}=[\alpha_1\mathcal{O}_\Delta\cap\mathcal{O}_{\Delta d^2}]^{(+)}\,[\beta\mathcal{O}_\Delta\cap\mathcal{O}_{\Delta d^2}]^{(+)}\,,$$

and therefore $[\alpha\mathcal{O}_\Delta\cap\mathcal{O}_{\Delta d^2}]^{(+)}=[\alpha_1\mathcal{O}_\Delta\cap\mathcal{O}_{\Delta d^2}]^{(+)}$. □[**A.**]

If $\alpha\in\mathcal{O}_\Delta$, then $\mathcal{N}(\alpha+Nd)=\mathcal{N}(\alpha)+Nd\mathcal{T}(\alpha)+N^2d^2>0$ for all sufficiently large $N\in\mathbb{N}$, and therefore $\mathcal{O}_\Delta/d\mathcal{O}_\Delta=\{\alpha+d\mathcal{O}_\Delta\mid\mathcal{N}(\alpha)>0\}$.

By **A**, there exists a group homomorphism $\vartheta^{(+)}\colon(\mathcal{O}_\Delta/d\mathcal{O}_\Delta)^\times\to\mathcal{C}^{(+)}_{\Delta d^2}$ such that $\vartheta^{(+)}(\alpha+d\mathcal{O}_\Delta)=[\alpha\mathcal{O}_\Delta\cap\mathcal{O}_{\Delta d^2}]^{(+)}$ for all $\alpha\in\mathcal{O}_\Delta$ satisfying $(\alpha,d)=1$ (and $\mathcal{N}(\alpha)>0$). We assert that

$$\mathrm{Ker}(\vartheta^{(+)})=\{a\varepsilon+d\mathcal{O}_\Delta\in(\mathcal{O}_\Delta/d\mathcal{O}_\Delta)^\times\mid a\in\mathbb{Z},\ (a,d)=1,\ \varepsilon\in\mathcal{O}^{\times(+)}_{\Delta}\,\}\,.$$

If $a \in \mathbb{Z}$ is such that $(a,d)=1$ and $\varepsilon \in \mathcal{O}_\Delta^{\times(+)}$, then $a\varepsilon + d\mathcal{O}_\Delta \in (\mathcal{O}_\Delta/d\mathcal{O}_\Delta)^\times$, ($\mathcal{N}(a\varepsilon)=a^2>0$), and $\vartheta^{(+)}(a\varepsilon+d\mathcal{O}_\Delta)=[a\varepsilon\mathcal{O}_\Delta\cap\mathcal{O}_{\Delta d^2}]^{(+)}$. Since

$$a\varepsilon\mathcal{O}_\Delta\cap\mathcal{O}_{\Delta d^2}=(a\mathcal{O}_\Delta\cap\mathcal{O}_{\Delta d^2})(\varepsilon\mathcal{O}_\Delta\cap\mathcal{O}_{\Delta d^2})=a\mathcal{O}_{\Delta d^2}\sim_+\mathcal{O}_{\Delta d^2}\,,$$

we obtain $a\varepsilon+d\mathcal{O}_\Delta\in\operatorname{Ker}(\vartheta^{(+)})$.

To prove the reverse inclusion, suppose that $a\in\mathbb{Z}$, $(a,d)=1$, $\varepsilon\in\mathcal{O}_\Delta^{\times(+)}$ and $[a\varepsilon\mathcal{O}_\Delta\cap\mathcal{O}_{\Delta d^2}]^{(+)}=[\mathcal{O}_{\Delta d^2}]^{(+)}$. Then there exists some $\beta\in\mathcal{O}_{\Delta d^2}^{(d)}$ such that $\alpha\mathcal{O}_\Delta=\beta\mathcal{O}_\Delta$ (and $\mathcal{N}(\beta)>0$), and therefore $\alpha=\beta\varepsilon$ for some $\varepsilon\in\mathcal{O}_\Delta^{\times(+)}$. Since $\mathcal{O}_{\Delta d^2}=[1,d\omega_\Delta]$, we obtain $\beta=a+bd\omega_\Delta$, where $a,\,b\in\mathbb{Z}$ and $(a,d)=1$, and therefore $\alpha+d\mathcal{O}_\Delta=a\varepsilon+bd\varepsilon+d\mathcal{O}_\Delta=a\varepsilon+d\mathcal{O}_\Delta$.

For the calculation of $|\operatorname{Ker}(\vartheta^{(+)})|$, let $\rho\colon(\mathbb{Z}/d\mathbb{Z})^\times\to\operatorname{Ker}(\vartheta^{(+)}$ be defined by $\rho(a+d\mathbb{Z})=a+d\mathcal{O}_\Delta$ for all $a\in\mathbb{Z}$ such that $(a,d)=1$. As $d\mathcal{O}_\Delta\cap\mathbb{Z}=d\mathbb{Z}$, it follows that ρ is monomorphism. By definition, the map $\varphi\colon\mathcal{O}_\Delta^{\times(+)}\to\operatorname{Ker}(\vartheta^{(+)})/\operatorname{Im}(\rho)$, defined by $\varphi(\varepsilon)=(\varepsilon+d\mathcal{O}_\Delta)\operatorname{Im}(\rho)$, is an epimorphism, and

$$\operatorname{Ker}(\varphi)=\{\varepsilon\in\mathcal{O}_\Delta^{\times(+)}\mid\varepsilon+d\mathcal{O}_\Delta\in\mathbb{Z}+d\mathcal{O}_\Delta=\mathcal{O}_{\Delta d^2}\}=\mathcal{O}_{\Delta d^2}^{\times(+)}\,.$$

Hence φ induces an isomorphism $\mathcal{O}_\Delta^{\times(+)}/\mathcal{O}_{\Delta d^2}^{\times(+)}\overset{\sim}{\to}\operatorname{Ker}(\vartheta^{(+)}/\operatorname{Im}(\rho)$, and we obtain

$$|\operatorname{Ker}(\vartheta^{(+)}|=|\operatorname{Im}(\rho)|(\mathcal{O}_\Delta^{\times(+)}:\mathcal{O}_{\Delta d^2}^{\times(+)})=\varphi(d)(\mathcal{O}_\Delta^{\times(+)}:\mathcal{O}_{\Delta d^2}^{\times(+)})\,.$$

3. For the exact sequence, it remains to prove that $\operatorname{Im}(\vartheta^{(+)})=\operatorname{Ker}(\Psi^{(+)})$. If $\alpha\in\mathcal{O}_\Delta$, $(\alpha,d)=1$ (and $\mathcal{N}(\alpha)>0$), then

$$\begin{aligned}\Psi^{(+)}\circ\vartheta^{(+)}(\alpha+d\mathcal{O}_\Delta)&=\Psi^{(+)}([\alpha\mathcal{O}_\Delta\cap\mathcal{O}_{\Delta d^2}]^{(+)})=[(\alpha\mathcal{O}_\Delta\cap\mathcal{O}_{\Delta d^2})\mathcal{O}_\Delta]^{(+)}\\&=[\alpha\mathcal{O}_\Delta]^{(+)}=[\mathcal{O}_\Delta]^{(+)}\,,\end{aligned}$$

and thus $\operatorname{Im}(\vartheta^{(+)})\subset\operatorname{Ker}(\Psi^{(+)})$. To prove the reverse inclusion, let $\mathfrak{a}\in\mathcal{J}_{\Delta d^2}^{(d)}$ be an $\mathcal{O}_{\Delta d^2}$-regular ideal such that $\Psi^{(+)}([\mathfrak{a}]^{(+)})=[\mathfrak{a}\mathcal{O}_\Delta]^{(+)}=[\mathcal{O}_\Delta]^{(+)}$. Then there exists some $\alpha\in\mathcal{O}_\Delta$ such that $(\alpha,d)=1$, $\mathfrak{a}\mathcal{O}_\Delta=\alpha\mathcal{O}_\Delta$ (and $\mathcal{N}(\alpha)>0$). Thus we obtain $[\mathfrak{a}]^{(+)}=[\alpha\mathcal{O}_\Delta\cap\mathcal{O}_{\Delta d^2}]^{(+)}=\vartheta^{(+)}(\alpha+d\mathcal{O}_\Delta)$.

From the exact sequence we deduce (using 2. and Theorem A.1.3)

$$h_{\Delta d^2}^{(+)}=h_\Delta^{(+)}\frac{|(\mathcal{O}_\Delta/d\mathcal{O}_\Delta)^\times|}{|\operatorname{Ker}(\vartheta^{(+)})|}=h_\Delta^{(+)}\,\frac{|(\mathcal{O}_\Delta/d\mathcal{O}_\Delta)^\times|}{\varphi(d)\,(\mathcal{O}_\Delta^{\times(+)}:\mathcal{O}_{\Delta d^2}^{\times(+)})}\,.$$

By Theorem 5.9.4 and Theorem A.6.2 it follows that

$$\frac{|(\mathcal{O}_\Delta/d\mathcal{O}_\Delta)^\times|}{\varphi(d)}=d\prod_{p\,|\,d}\Bigl(1-\frac{\mathsf{Q}_\Delta(p)}{p}\Bigr)\,,$$

which implies the final formula. □

We remark that the unit index $(\mathcal{O}_\Delta^{\times(+)}:\mathcal{O}_{\Delta d^2}^{\times(+)})$ in Theorem 5.9.7 is easy to handle. Indeed, if $q\in\mathbb{N}$ is minimal such that $\varepsilon_\Delta^q\in\mathcal{O}_{\Delta d^2}$, then $(\mathcal{O}_\Delta^\times:\mathcal{O}_{\Delta d^2}^\times)=q$, and $(\mathcal{O}_\Delta^{\times+}:\mathcal{O}_{\Delta d^2}^{\times+})=\dfrac{q}{2}$ if $\mathcal{N}(\varepsilon_\Delta)=-1$ and $2\,|\,q$, and $(\mathcal{O}_\Delta^{\times+}:\mathcal{O}_{\Delta d^2}^{\times+})=q$ otherwise.

Exercise 5.9.8. Let Δ be a quadratic discriminant, p a prime and

$$\varepsilon_\Delta^{(+)} = \frac{u+v\sqrt{\Delta}}{2}\,, \quad \text{where} \quad u,\,v\in\mathbb{N}\,,\ u\equiv v\Delta \bmod 2 \ \text{ and } \ p\,|\,v\,.$$

Prove that $h_{\Delta p^2}^{(+)} = ph_\Delta^{(+)}$.

Another interesting special case of Theorem 5.9.7 (dealt with in the following Corollary 5.9.9) occurs when $\Delta\equiv 1 \bmod 4$ and $d=2$. This case plays an important role in Mertens' proof of Gauss' duplication theorem (see Theorem 6.5.11).

Corollary 5.9.9. *Let* $\Delta\equiv 1 \bmod 4$ *be a quadratic discriminant, and let*

$$\Psi^{(+)} = \Psi_{\Delta,2}^{(+)}\colon \mathcal{C}_{4\Delta}^{(+)} \ \to\ \mathcal{C}_\Delta^{(+)}$$

be the epimorphism defined by $\Psi^{(+)}([\mathfrak{a}]^{(+)}) = [\mathfrak{a}\mathcal{O}_\Delta]^{(+)}$ *for all* $\mathcal{O}_{4\Delta}$*-regular ideals* $\mathfrak{a}\in\mathcal{I}_{4\Delta}^{(2)}$ (see Theorem 5.9.7). *Then*

$$|\mathrm{Ker}(\Psi_\Delta^{(+)})| = \begin{cases} 3 & \textit{if} \quad \Delta\equiv 5 \bmod 8 \quad \textit{and} \quad \mathcal{O}_\Delta^\times = \mathcal{O}_{4\Delta}^\times\,, \\ 1 & \textit{otherwise.}\end{cases}$$

Explicitly, if $\Delta\equiv 5 \bmod 8$, *then*

$$\mathfrak{a} = \Big[\frac{1-\Delta}{4}, 1+\sqrt{\Delta}\Big] \quad \textit{is an } \mathcal{O}_{4\Delta}\textit{-regular ideal,} \quad \mathfrak{a}\mathcal{O}_\Delta = \frac{1+\sqrt{\Delta}}{2}\,\mathcal{O}_\Delta\,,$$

and $\mathfrak{a}$ *is a principal ideal of* $\mathcal{O}_{4\Delta}$ *if and only if* $\mathcal{O}_\Delta^\times \ne \mathcal{O}_{4\Delta}^\times$.

Proof. By Theorem 5.9.7,

$$|\mathrm{Ker}(\Psi^{(+)}| = |\mathrm{Im}(\vartheta^{(+)}| = \frac{|(\mathcal{O}_\Delta/2\mathcal{O}_\Delta)^\times|}{|\mathrm{Ker}(\vartheta^{(+)})|} = \frac{|(\mathcal{O}_\Delta/2\mathcal{O}_\Delta)^\times|}{(\mathcal{O}_\Delta^{\times(+)}\!:\!\mathcal{O}_{4\Delta}^{\times(+)})}\,.$$

CASE 1: $\Delta\equiv 1 \bmod 8$. In this case, $2\mathcal{O}_\Delta = \mathfrak{p}\mathfrak{p}'$, where $\mathfrak{p}$, $\mathfrak{p}'$ are $\mathcal{O}_\Delta$-regular prime ideals, $\mathfrak{p}\ne\mathfrak{p}'$, $\mathfrak{N}_\Delta(\mathfrak{p}) = \mathfrak{N}_\Delta(\mathfrak{p}') = 2$, and $|(\mathcal{O}_\Delta/2\mathcal{O}_\Delta)^\times| = 1$ by Theorem 5.9.3. Hence it follows that $|\mathrm{Ker}(\Psi^{(+)})| = 1$.

CASE 2: $\Delta\equiv 5 \bmod 8$. In this case, $2\mathcal{O}_\Delta$ is a prime ideal, $|(\mathcal{O}_\Delta/2\mathcal{O}_\Delta)^\times| = 3$, and therefore $|\mathrm{Ker}(\Psi^{(+)})| = 1$ if and only if $\mathcal{O}_\Delta^{\times(+)} \ne \mathcal{O}_{4\Delta}^{\times(+)}$.

If $\Delta < -3$, then $\mathcal{O}_\Delta^\times = \mathcal{O}_{4\Delta}^\times$. If $\Delta=-3$, then $\zeta_3\in\mathcal{O}_\Delta^\times\setminus\mathcal{O}_{4\Delta}^\times$. If $\Delta>0$, then $(\mathcal{O}_\Delta^\times:\mathcal{O}_{4\Delta}^\times)\in\{1,3\}$ by Theorem 5.2.3.1, and therefore $\mathcal{O}_\Delta^\times = \mathcal{O}_{4\Delta}^\times$ if and only if $\mathcal{O}_\Delta^{\times+} = \mathcal{O}_{4\Delta}^{\times+}$.

Now we consider the $\mathcal{O}_\Delta$-regular ideal

$$\mathfrak{a} = \Big[\frac{1-\Delta}{4}, 1+\sqrt{\Delta}\Big]\,.$$

By Theorem 5.9.5 we obtain

$$\mathfrak{a}\mathcal{O}_\Delta = \Big[\frac{1-\Delta}{4}, \frac{1+\sqrt{\Delta}}{2}\Big] = \frac{1+\sqrt{\Delta}}{2}\,\mathcal{O}_\Delta\,,$$

and therefore $[\mathfrak{a}]\in\mathrm{Ker}(\Psi)$. If $\mathcal{O}_\Delta^\times \ne \mathcal{O}_{4\Delta}^\times$, then Ψ is an isomorphism, and thus $\mathfrak{a}$ is a principal ideal of $\mathcal{O}_\Delta$.

Assume now that $\mathfrak{a}$ is a principal ideal of $\mathcal{O}_{4\Delta}$. Then

$$\mathfrak{a} = I\Big(\frac{4(1+\sqrt{\Delta})}{1-\Delta}\Big) \sim I(\sqrt{\Delta}\,), \quad \text{and therefore} \quad \frac{4(1+\sqrt{\Delta})}{1-\Delta} \sim \sqrt{\Delta}\,.$$

Let α, β, γ, $\delta \in \mathbb{Z}$ be such that $|\alpha\delta-\beta\gamma| = 1$ and

$$\frac{4(1+\sqrt{\Delta})}{1-\Delta} = \frac{\alpha\sqrt{\Delta}+\beta}{\gamma\sqrt{\Delta}+\delta}\,.$$

Then it follows that $4\delta+4\gamma\Delta = (1-\Delta)\beta$ and $4\delta+4\gamma = (1-\Delta)\alpha$, which implies

$$\gamma = \frac{\alpha-\beta}{4}\,, \quad \delta = \frac{(1-\Delta)\alpha-(\alpha-\beta)}{4} \quad \text{and} \quad 1 = |\alpha\delta-\beta\gamma| = \frac{\beta^2-\Delta\alpha^2}{4}\,.$$

Hence $|\beta^2-\Delta\alpha^2| = 4$ and $(\beta,\alpha) = 1$, which implies that

$$\frac{\beta+\alpha\sqrt{\Delta}}{2} \in \mathcal{O}_\Delta^\times \setminus \mathcal{O}_{4\Delta}^\times\,. \qquad \square$$

Example 5.9.10. We close this section with an amusing connection between class numbers and the Fibonacci sequence $(F_n)_{n\ge 0}$, recursively defined by

$$F_0 = 0\,, \quad F_1 = 1 \quad \text{and} \quad F_n = F_{n-1}+F_{n-2} \quad \text{for all } n \ge 2\,.$$

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
F_n	0	1	1	2	3	5	8	13	21	34	55	89	144	233	377	619	987

Recall from Chapter 3 that

$$\varepsilon_5 = \omega_5 = \frac{1+\sqrt{5}}{2}\,, \quad l(\varepsilon_5) = 1 \quad \text{and} \quad \varepsilon_5 = [\,\overline{1}\,]\,.$$

If $(p_n)_{n\ge -2}$ denotes the sequence of partial numerators and $(q_n)_{n\ge -2}$ the sequence of partial denominators of ε_5, then $F_n = p_{n-2} = q_{n-1}$ for all $n \in \mathbb{N}_0$. In particular, Theorem 2.1.1 implies $(F_n, F_{n+1}) = 1$,

$$\begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n \quad \text{for all } n \in \mathbb{N}, \text{ and } \lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \varepsilon_5\,.$$

By Theorem 2.3.5 we obtain $\varepsilon_5^m = F_{m+1} - F_m\varepsilon_5'$ for all $m \in \mathbb{N}_0$, hence

$$\varepsilon_5^m - \varepsilon_5'^m = (F_{m+1}-F_m\varepsilon_5') - (F_{m+1}-F_m\varepsilon_5) = F_m(\varepsilon_5-\varepsilon_5') = F_m\sqrt{5}\,,$$

and the well-known formula

$$F_m = \frac{1}{\sqrt{5}}\,(\varepsilon_5^m - \varepsilon_5'^m) = \frac{1}{2^{m-1}}\sum_{j=0}^{\infty}\binom{m}{2j+1}5^j \quad \text{for all } m \ge 1.$$

For $d \in \mathbb{N}$, we consider the order $\mathcal{O}_{5d^2} = [1, d\omega_5']$. If $n \in \mathbb{N}$, then $\varepsilon_5^n \in \mathcal{O}_{5d^2}$ if and only if $d \,|\, F_n$, and we define

$$\kappa(d) = (\mathcal{O}_5^\times : \mathcal{O}_{5d^2}^\times) = \min\{n \in \mathbb{N} \mid F_n \equiv 0 \bmod d\}\,.$$

It follows that $\{n \in \mathbb{N} \mid F_n \equiv 0 \bmod d\} = \kappa(d)\mathbb{N}_0$, and by Theorem 5.9.7 we obtain

$$h_{5d^2} = \frac{d}{\kappa(d)} \prod_{p \,|\, d} \Big(1 - \frac{\mathsf{Q}_5(p)}{p}\Big), \quad \text{where} \quad \mathsf{Q}_5(p) = \Big(\frac{5}{p}\Big) = \begin{cases} 1 & \text{if} \quad p \equiv \pm 1 \mod 5\,, \\ -1 & \text{if} \quad p \equiv \pm 2 \mod 5\,. \end{cases}$$

The following simple Lemma 5.9.11 should be well known to experts in Fibonacci numbers. I state it with proof for lack of a suitable reference.

Lemma 5.9.11. *Let p be a prime.*

1. $\kappa(p) \,|\, p-1$ *if* $p \equiv \pm 1 \bmod 5$, *and* $\kappa(p) \,|\, p+1$ *if* $p \equiv \pm 2 \bmod 5$.
2. *If* $n \in \mathbb{N}$ *and* $\kappa(p) \nmid n$, *then* $p \nmid F_n$.
3. *If* $n = \kappa(p)p^e l$, *where* $e \in \mathbb{N}_0$, $l \in \mathbb{N}$ *and* $p \nmid l$, *then* $\mathsf{v}_p(F_n) = \nu(p) + e + \eta$, *where*

$$\nu(p) = \mathsf{v}_p(F_{\kappa(p)}) \quad \textit{and} \quad \eta = \begin{cases} 1 & \textit{if} \quad p = 2 \quad \textit{and} \quad m \geq 1\,, \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. 1. Since $\kappa(p) = (\mathcal{O}_5^\times : \mathcal{O}_{5p^2}^\times)$, and

$$h_{5p^2} = \frac{p}{\kappa(p)} \Big(1 - \frac{\mathsf{Q}_5(p)}{p}\Big) = \frac{p - \mathsf{Q}_5(p)}{\kappa(p)}\,,$$

we infer $\kappa(p) \,|\, p - \mathsf{Q}_5(p)$ (recall that $\mathsf{Q}_5(p) = 1$ if $p \equiv \pm 1 \bmod 5$, and $\mathsf{Q}_5(p) = -1$ if $p \equiv \pm 2 \bmod 5$).

2. If $n \in \mathbb{N}$ and $\kappa(p) \nmid n$, then $\varepsilon_5^n \notin \mathcal{O}_{5p^2}^\times$, and therefore $p \nmid F_n$.

3. We proceed by induction on n. From the table above, we see that $\kappa(2) = 3$, $\nu(2) = 1$ and $\mathsf{v}_2(F_6) = 3$. Hence it suffices to prove the following assertion:

A. If $N \in \mathbb{N}$ and $\mathsf{v}_p(F_N) = k \geq 1$, then

- $\mathsf{v}_p(F_{lN}) = k$ for all $l \in \mathbb{N}$ such that $p \nmid l$, and
- $\mathsf{v}_p(F_{pN}) = k+1$ unless $p = 2$ and $k = 1$.

Proof of **A.** Let $N \in \mathbb{N}$, and suppose that $\mathsf{v}_p(F_N) = k \geq 1$. We set $F_N = p^k a$ and $F_{N-1} = b$, where $a, b \in \mathbb{N}$ and $p \nmid ab$. Then

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^N = \begin{pmatrix} F_{N+1} & F_N \\ F_N & F_{N-1} \end{pmatrix} = \begin{pmatrix} F_N + F_{N-1} & F_N \\ F_N & F_{N-1} \end{pmatrix} = \begin{pmatrix} p^k a + b & p^k a \\ p^k a & b \end{pmatrix}\,,$$

and for $l \in \mathbb{N}$ we get

$$\begin{pmatrix} F_{Nl+1} & F_{Nl} \\ F_{Nl} & F_{Nl-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{Nl} = \begin{pmatrix} p^k a + b & p^k a \\ p^k a & b \end{pmatrix}^l\,.$$

By induction on $l \geq 1$, we obtain the following congruence modulo p^{3k}:

$$\begin{pmatrix} p^k a + b & p^k a \\ p^k a & b \end{pmatrix}^l \equiv \begin{pmatrix} l(l-1)p^{2k}a^2b^{l-2} + lp^k ab^{l-1} + b^l & \frac{l(l-1)}{2}\, p^{2k}a^2b^{l-2} + lp^k ab^{l-1} \\ \frac{l(l-1)}{2}\, p^{2k}a^2b^{l-2} + lp^k ab^{l-1} & \frac{l(l-1)}{2}\, p^{2k}a^2b^{l-2} + b^l \end{pmatrix}\,.$$

In particular, for all $l \geq 2$ it follows that

$$F_{lN} \equiv p^k ab^{l-2}\Big(\frac{l(l-1)}{2}\, p^k a + lb\Big) \mod p^{3k}\,.$$

If $p \nmid l$, this implies $\mathsf{v}_p(F_{lN}) = k$. Moreover, we obtain

$$F_{pN} \equiv p^{k+1} a b^{p-2} \Big(\frac{p-1}{2}\, p^k + b \Big)\,,$$

and therefore $\mathsf{v}_p(F_{pN}) = k+1$ unless $p=2$ and $k=1$. □

Dijana Kreso (private communication) observed that $\nu(p) \le \overline{\nu}(p) = \mathsf{v}_p(F_{l(p)})$, where $l(p)$ denotes the period length of the Fibonacci sequence modulo p. The numbers $l(p)$ and $\overline{\nu}(p)$ were investigated in [**105**]. There it was conjectured that $\overline{\nu}(p) = 1$ for all primes p, and this has been verified for all primes $p < 2 \cdot 10^{14}$ in [**71**].

From the table above we see that $\kappa(5) = 5$, $\kappa(2) = 3$, and $\nu(5) = \nu(2) = 1$.

Now we can state the announced connection between Fibonacci numbers and class numbers. In particular, the following theorem also produces infinitely many quadratic discriminants with class number 1 (see [**117**, §9, Aufgabe 5]).

Theorem 5.9.12. *Let p be an odd prime and $n \in \mathbb{N}$. Then*

$$(\mathcal{O}_5^\times : \mathcal{O}_{5p^{2n}}^\times) = \kappa(p)\, p^{\max\{n-\nu(p),0\}} \quad \textit{and} \quad h_{5p^{2n}} = p^{\min\{\nu(p),n\}-1}\, \frac{p - \mathsf{Q}_5(p)}{\kappa(p)}\,.$$

In particular, $h_{5^{2n+1}} = 1$.

Proof. If $m = (\mathcal{O}_5^\times : \mathcal{O}_{5p^{2n}}^\times)$, then m is the smallest positive integer such that $F_m \equiv 0 \mod p^n$. Now Lemma 5.9.11 implies that $\kappa(p) \mid m$, and if $m = \kappa(p) p^e l$, where $e \in \mathbb{N}_0$, $l \in \mathbb{N}$ and $p \nmid l$, then $n = \nu(p) + e$. Consequently, the smallest $m \in \mathbb{N}$ such that $\mathsf{v}_p(F_m) \ge n$ is $m = \kappa(p) p^e$, where $e = \max\{n - \nu(p), 0\}$.

The formula for $h_{5p^{2n}}$ follows by Theorem 5.9.7. Since $\kappa(5) = 5$ and $\nu(5) = 1$, we obtain $(\mathcal{O}_5^\times : \mathcal{O}_{5^{2n+1}}^\times) = 5^n$, and $h_{5^{2n+1}} = 1$. □

Exercise 5.9.13. Prove that $h_{20} = h_{80} = 1$, and $h_{5\cdot 2^{2n}} = 2$ for all $n \ge 3$. Calculate $h^+_{5\cdot 2^{2n}}$ for all $n \in \mathbb{N}$.

Exercise 5.9.14. For $n \in \mathbb{N}$ and an odd prime p, derive a formula for $h^+_{5p^{2n}}$.

CHAPTER 6

Binary quadratic forms

In this chapter we prove the main theorems of Gauss' theory of binary quadratic forms and connect it with the ideal theory of quadratic orders and the theory of continued fractions. Thereby the close connection between the various concepts of the theory of quadratic irrationals becomes apparent.

We tacitly use the properties of quadratic residues and quadratic characters as developed in Chapter 3.

6.1. Elementary definitions and equivalence relations

An (*integral binary quadratic*) *form* is a homogeneous quadratic polynomial $f \in \mathbb{Z}[X,Y]$, and we write it in the form

$$f = [a,b,c] = aX^2 + bXY + cY^2 \in \mathbb{Z}[X,Y]\,.$$

We call $\Delta_f = b^2 - 4ac$ the *discriminant* of f, $d_f = (a,b,c) \in \mathbb{N}_0$ the *divisor* of f, and

$$M_f = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \in \mathsf{M}_2(\mathbb{Q})\,,$$

the *matrix* of f. By definition,

$$f = (X\,Y)\,M_f \begin{pmatrix} X \\ Y \end{pmatrix}, \quad \Delta_f = -4\det(M_f)\,, \quad d_f^2 \mid \Delta_f\,,$$

and $d_f = 0$ if and only if $f = 0$.

A form $f = [a,b,c]$ is with discriminant Δ_f and divisor d_f is called

- *degenerate* if Δ_f is a square, otherwise *non-degenerate*;
- *primitive* if $d_f = 1$.

If $f = [a,b,c]$ is a non-degenerate form, then $ac \ne 0$, Δ_f is a quadratic discriminant, and we define the *root* of f by

$$\xi_f = \frac{b + \sqrt{\Delta_f}}{2a} \in \mathbb{C}\,.$$

Then $f = a(X + \xi_f Y)(X + \xi_f' Y)$, and as $a\xi_f^2 - b\xi_f + c = 0$, it follows that ξ_f is a quadratic irrational of type $(d_f^{-1}a, d_f^{-1}b, d_f^{-1}c)$ and discriminant $d_f^{-2}\Delta_f$. In particular, d_f divides the conductor of Δ_f, and if Δ_f is a fundamental discriminant, then f is primitive.

A non-degenerate form f is uniquely determined by its root ξ_f and its divisor d_f. Indeed, it ξ_f is of type (a_0, b_0, c_0), then $f = [d_f a_0, d_f b_0, d_f c_0]$.

In particular: If Δ is a quadratic discriminant and d is a positive divisor of its conductor f_Δ, then the assignment $f \mapsto \xi_f$ defines a bijective map from the set of all forms with discriminant Δ and divisor d onto the set of all quadratic irrationals of discriminant Δ.

If $f = [a, b, c]$ is a form and m is an integer, then we say that

- f *represents* m if there exist $x,\ y \in \mathbb{Z}$ such that
$$m = f(x, x) = ax^2 + bxy + cy^2 = (x\,y)M_f \begin{pmatrix} x \\ y \end{pmatrix};$$
- f *properly represents* m if there exist $x,\ y \in \mathbb{Z}$ such that $(x, y) = 1$ and $m = f(x, y)$.

If f (properly) represents m, then we also say that m is (*properly*) *represented* by f. By definition, f (properly) represents m if and only if $d_f \mid m$ and the primitive form $d_f^{-1}f$ (properly) represents $d_f^{-1}m$. Consequently, if f represents m and $(\Delta_f, m) = 1$, then f is primitive.

For a given form f, it is a fundamental problem to determine all integers which are (properly) represented by f. For example, a positive integer is the sum of two (coprime) integral squares if and only if it is (properly) represented by the form $[1, 0, 1]$. In its full generality, this problem (at least for primes) is equivalent to the problem of prime decomposition laws for ring class fields, a topic of higher algebraic number theory which is beyond the scope of this book.

The main work in establishing the theory presented in this chapter was already done by C. F. Gauss, and we cordially recommend the reader to consult the reprint of Gauss' original work [**32**] as well as the exposition of P. G. L. Dirichlet made sixty years later [**23**]. In our presentation of the theory, we place emphasis on the connection with the theory of quadratic irrationals and the theory of quadratic orders.

A form $f = [a, b, c]$ is called

- *positive definite* if $\Delta_f < 0$ and $a > 0$;
- *negative definite* if $\Delta_f < 0$ and $a < 0$;
- *indefinite* if it is non-degenerate and $\Delta_f > 0$.

A non-degenerate form f is positive definite if $\Im(\xi_f) > 0$, negative definite if $\Im(\xi_f) < 0$, and indefinite if $\xi_f \in \mathbb{R}$. By definition, f is positive definite if and only if $-f$ is negative definite.

Lemma 6.1.1. *Let f be a form.*

1. *f is degenerate if and only if f properly represents 0.*
2. *If $\Delta_f > 0$, then there exist integers $x_1,\ x_2 \in \mathbb{Z}$ and $y \in \mathbb{N}$ such that*
$$(x_1, y) = (x_2, y) = 1 \quad \textit{and} \quad f(x_1, y)f(x_2, y) < 0\,.$$
In particular, f properly represents positive and negative integers.
3. *f is positive [negative] definite if and only if $f(x, y) > 0$ [$f(x, y) < 0$] for all $(x, y) \in \mathbb{Z}^2 \setminus \{(0, 0)\}$.*

PROOF. Suppose that $f = [a, b, c]$.

1. If f is non-degenerate, then $a \neq 0$, ξ_f is a quadratic irrational, and

$$f(x,y) = a(x+\xi_f y)(x+\xi_f' y) \neq 0 \quad \text{for all} \quad (x,y) \in \mathbb{Z}^2 \setminus \{(0,0)\}\,.$$

Hence f does not properly represent 0.

If f is degenerate and $a = 0$, then $f(1,0) = 0$. If f is degenerate and $a \neq 0$, then $f(b, -2a) = ab^2 - 2ab^2 + 4a^2c = -a\Delta_f = 0$, and since we may cancel the greatest common divisor of b and $2a$, it follows that f properly represents 0.

2. CASE 1: $a = 0$. Then $b \neq 0$, and $f(x,y) = y(bx+cy)$ for all $(x,y) \in \mathbb{Z}^2$. If x_1, $x_2 \in \mathbb{Z}$ are such that $bx_1 + c > 0$ and $bx_2 + c < 0$, then $f(x_1, 1) > 0$ and $f(x_2, 1) < 0$.

CASE 2: $a \neq 0$. Then

$$f = a\Big[X + \frac{b+\sqrt{\Delta_f}}{2a}\,Y\Big]\Big[X + \frac{b-\sqrt{\Delta_f}}{2a}\,Y\Big]\,,$$

and there exist integers x_1, $x_2 \in \mathbb{Z}$ and $y \in \mathbb{N}$ such that $(x_1, y) = (x_2, y) = 1$,

$$\Big(\frac{x_1}{y} + \frac{b+\sqrt{\Delta}}{2a}\Big)\Big(\frac{x_1}{y} + \frac{b-\sqrt{\Delta}}{2a}\Big) < 0\,, \quad \Big(\frac{x_2}{y} + \frac{b+\sqrt{\Delta}}{2a}\Big)\Big(\frac{x_2}{y} + \frac{b-\sqrt{\Delta}}{2a}\Big) > 0\,,$$

and consequently $f(x_1, y)f(x_2, y) < 0$.

3. If f is positive or negative definite, then $\Delta_f < 0$, $\xi_f' = \overline{\xi_f}$, and

$$f(x,y) = a\,|x + \xi_f y|^2 \gtrless 0 \quad \text{for all } (x,y) \in \mathbb{Z} \setminus \{(0,0)\} \text{ if } \quad a \gtrless 0\,.$$

If f is neither positive nor negative definite, then $\Delta_f \le 0$, and the assertion follows by 1. and 2. $\square$

For a form $f = [a, b, c]$, we define the forms $-f$, f^- and f^{op} by

$$-f = [-a, -b, -c]\,, \quad f^- = [-a, b, -c] \quad \text{and} \quad f^{\mathsf{op}} = [a, -b, c]\,.$$

By definition, we get $\Delta_f = \Delta_{-f} = \Delta_{f^-} = \Delta_{f^{\mathsf{op}}}$, $d_f = d_{-f} = d_{f^{-1}} = d_{f^{\mathsf{op}}}$, and $(-f)(x,y) = -f(x,y)$, $f^-(x,y) = -f(x,-y)$, $f^{\mathsf{op}}(x,y) = f(x,-y)$ for all x, $y \in \mathbb{Z}$. In particular, f and f^{op} (properly) represent the same integers, and f (properly) represents some $m \in \mathbb{Z}$ if and only if $-f$ (resp. f^-) (properly) represents $-m$. If f is non-degenerate, then $\xi_{-f} = \xi_f'$, $\xi_{f^-} = -\xi_f$, and $\xi_{f^{\mathsf{op}}} = -\xi_f'$.

For a quadratic discriminant $\Delta = 4D + \sigma$, where $D \in \mathbb{Z}$ and $\sigma \in \{\pm 1\}$, we call

$$g_\Delta = [1, \sigma, -D]$$

the *principal form* of discriminant Δ. Its root $\xi_{g_\Delta} = \omega_\Delta = (\sigma + \sqrt{\Delta}\,)/2$ is the basis number of discriminant Δ. If $\Delta < 0$, then g_Δ is positive definite.

In the following definition we formalize the procedure of transforming one form into another one by a unimodular change of variables. This gives rise to an equivalence relation on the set of forms of given discriminant such that equivalent forms (properly) represent the same integers with the same multiplicity.

Definition 6.1.2. For a form $f=[a,b,c]=aX^2+bXY+cY^2\in\mathbb{Z}[X,Y]$ and a matrix

$$A=\begin{pmatrix}\alpha&\beta\\ \gamma&\delta\end{pmatrix}\in\mathsf{M}_2(\mathbb{Z})$$

we define $Af\in\mathbb{Z}[X,Y]$ by

$$\begin{aligned}Af&=f(\alpha X+\gamma Y,\beta X+\delta Y)\\ &=a(\alpha X+\gamma Y)^2+b(\alpha X+\gamma Y)(\beta X+\delta Y)+c(\beta X+\delta Y)^2\\ &=(\alpha X+\gamma Y\ \ \beta X+\delta Y)\,M_f\begin{pmatrix}\alpha X+\gamma Y\\ \beta X+\delta Y\end{pmatrix}=(X\,Y)\,A\,M_f\,A^{\mathsf{t}}\begin{pmatrix}X\\ Y\end{pmatrix}\\ &=a_1X^2+b_1XY+c_1Y^2\,,\end{aligned}$$

where

$$\begin{aligned}a_1&=a\alpha^2+b\alpha\beta+c\beta^2=f(\alpha,\beta)\,,\\ b_1&=2a\alpha\gamma+b(\alpha\delta+\beta\gamma)+2c\beta\delta\,,\\ c_1&=a\gamma^2+b\gamma\delta+c\delta^2=f(\gamma,\delta)\,.\end{aligned}$$

In particular, $Af=[a_1,b_1,c_1]$ is a form, and $d_f\,|\,d_{Af}$.

The following special cases will frequently be used: If $[a,b,c]$ is a form, then

$$[a,b,c]^{\mathsf{op}}=[a,-b,c]=\begin{pmatrix}-1&0\\ 0&1\end{pmatrix}[a,b,c]\,,\quad [c,-b,a]=\begin{pmatrix}0&1\\ -1&0\end{pmatrix}[a,b,c]\,,$$

and if $l\in\mathbb{Z}$, then

$$[a,\,b+2la,\,al^2+bl+c\,]=\begin{pmatrix}1&0\\ l&1\end{pmatrix}[a,b,c]\,.$$

If A, $B\in\mathsf{M}_2(\mathbb{Z})$ and f is a form, the it follows by the very definition that

$$Af=(-A)f\,,\quad M_{Af}=AM_fA^{\mathsf{t}}\,,\quad \Delta_{Af}=\det(A)^2\Delta_f\,,$$

and since $M_{A(Bf)}=AM_{Bf}A^{\mathsf{t}}=ABM_fB^{\mathsf{t}}A^{\mathsf{t}}=(AB)M_f(AB)^{\mathsf{t}}=M_{(AB)f}$, we get

$$(AB)f=A(Bf)\,.$$

Assume now that $A\in\mathsf{GL}_2(\mathbb{Z})$, and let f be a form. Then $\Delta_{Af}=\Delta_f$, and since $A^{-1}\in\mathsf{GL}_2(\mathbb{Z})$ and $A^{-1}(Af)=f$, it follows that $d_{Af}\,|\,d_f$, hence $d_f=d_{Af}$, and Af is primitive if and only if f is primitive. If x, $y\in\mathbb{Z}$ and $(x',\,y')=(x,\,y)A$, then

$$(Af)(x,y)=(x,\,y)M_{Af}\begin{pmatrix}x\\ y\end{pmatrix}=(x,\,y)AM_fA^{\mathsf{t}}\begin{pmatrix}x\\ y\end{pmatrix}=(x',y')M_f\begin{pmatrix}x'\\ y'\end{pmatrix}=f(x',y')\,.$$

Consequently, for every integer $m\in\mathbb{Z}$, the map

$$\Theta_{f,A}\colon\{(x,y)\in\mathbb{Z}^2\mid(Af)(x,y)=m\}\ \to\ \{(x',y')\in\mathbb{Z}^2\mid f(x',y')=m\,\}\,,$$

defined by $\Theta_{f,A}(x,y)=(x,y)A$, is bijective, and if $\Theta_{f,A}(x,y)=(x',y')$, then $(x,y)=1$ if and only if $(x',y')=1$. Hence $\Theta_{f,A}$ defines a bijective map from the set of all (proper) representations of m by Af onto the set of all (proper) representations of m by f.

Two forms f and g are called

- *equivalent*, $f\sim g$, if $g=Af$ for some matrix $A\in\mathsf{SL}_2(\mathbb{Z})$;

- *weakly equivalent* if $g = Af$ for some matrix $A \in \mathsf{GL}_2(\mathbb{Z})$;
- *improperly equivalent* if $g = Af$ for some matrix $A \in \mathsf{GL}_2(\mathbb{Z}) \setminus \mathsf{SL}_2(\mathbb{Z})$.

Equivalence and weak equivalence are equivalence relations. Weakly equivalent forms have the same discriminant, the same divisor, and they (properly) represent the same integers. Nonetheless, the subsequent Theorems 6.1.4 and 6.4.2 will show that equivalence is the more important notion since it matches with the corresponding definitions for quadratic irrationals and for ideals in quadratic orders.

By definition, f and f^{op} are improperly equivalent. Hence two forms f and g are improperly equivalent if and only if either $f \sim g$ or $f \sim g^{\mathsf{op}}$.

We start our investigation of the equivalence relation with the (rather trivial) case of degenerate forms.

Theorem 6.1.3. *Let f be a degenerate form and $n \in \mathbb{N}_0$ such that $\Delta_f = n^2$.*

1. *There exists some $l \in \mathbb{Z}$ such that $f \sim [0, n, l]$.*
2. *If l_1, $l_2 \in \mathbb{Z}$, then $[0, n, l_1] \sim [0, n, l_2]$ holds if and only if $l_1 \equiv l_2 \bmod n$.*

Proof. 1. Suppose that $f = [a, b, c]$. By Lemma 6.1.1 there exist x, $y \in \mathbb{Z}$ such that $(x, y) = 1$ and $f(x, y) = 0$. Then there exist u, $v \in \mathbb{Z}$ satisfying $xv - yu = 1$, and consequently

$$\begin{pmatrix} x & y \\ u & v \end{pmatrix} f = [0, n_1, l_1] \quad \text{for some } n_1,\ l_1 \in \mathbb{Z}\,, \quad \text{and} \quad n^2 = \Delta_f = n_1^2\,.$$

If $n_1 \geq 0$, then $n = n_1$, we set $l = l_1$, and we are done. Thus assume that $n_1 < 0$, set $d = (n_1, l_1)$, $n_1 = d\beta$ and $l_1 = -d\alpha$, where α, $\beta \in \mathbb{Z}$ and $(\alpha, \beta) = 1$. If γ, $\delta \in \mathbb{Z}$ are such that $\alpha\delta - \beta\gamma = 1$, then

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} [0, n_1, l_1] = [0, -n_1, l] = [0, n, l]$$

for some $l \in \mathbb{Z}$, and we are done again.

2. If l_1, $l_2 \in \mathbb{Z}$ and $l_1 \equiv l_2 \bmod n$, then $l_2 - l_1 = nk$ for some $k \in \mathbb{Z}$, and

$$\begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix} [0, n, l_1] = [0, n, l_2]\,.$$

As to the converse, assume that l_1, $l_2 \in \mathbb{Z}$ and

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} [0, n, l_1] = [0, n, l_2] \quad \text{for some matrix} \quad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathsf{SL}_2(\mathbb{Z})$$

satisfying (without restriction) $\delta \geq 0$. Then $0 = \beta(\alpha n + l_1\beta)$, $n = n + 2\beta(n\gamma + l_1\delta)$ and $l_2 = \delta(n\gamma + l_1\delta)$. If $\beta = 0$, then $\alpha = \delta = 1$ and $l_2 = l_1 + n\gamma \equiv l_1 \bmod n$. If $\beta \neq 0$, then $n\gamma + l_1\delta = 0$, hence $l_2 = 0$, and also $l_1 = l_1(\alpha\delta - \beta\gamma) = -n\alpha\gamma + \gamma\alpha n = 0$. □

Next we investigate the equivalence relation for non-degenerate forms. Our main tool is to compare the transformation of a non-degenerate form with the transformation of its root. We need the following definition. For a matrix

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathsf{M}_2(\mathbb{Z})\,, \quad \text{we define} \quad A^\dagger = \begin{pmatrix} \delta & \gamma \\ \beta & \alpha \end{pmatrix}\,.$$

It is easily checked that $A^{\dagger\dagger} = A$, $\det(A^\dagger) = \det(A)$, and $(AB)^\dagger = A^\dagger B^\dagger$ for all $A, B \in \mathsf{M}_2(\mathbb{Z})$. In particular, the assignment $A \mapsto A^\dagger$ defines automorphisms of $\mathsf{M}_2(\mathbb{Z})$, $\mathsf{GL}_2(\mathbb{Z})$ and $\mathsf{SL}_2(\mathbb{Z})$.

Theorem 6.1.4. *Let $f = [a,b,c]$ be a non-degenerate form and $A \in \mathsf{SL}_2(\mathbb{Z})$.*

1. *If $Af = [a_1, b_1, c_1]$, then $\xi_{Af} = A^\dagger \xi_f$, and $a_1 = a\mathcal{N}(\beta\xi_f + \alpha)$.*
2. *If g is another non-degenerate form, then $g = Af$ if and only if $\xi_g = A^\dagger \xi_f$ and $d_g = d_f$. In particular, f and g are equivalent if and only if $d_f = d_g$ and ξ_f and ξ_g are properly equivalent.*

PROOF. 1. By definition, we obtain

$$\begin{aligned} Af &= f(\alpha X + \gamma Y,\ \beta X + \delta Y) \\ &= a\big[(\alpha X + \gamma Y) + \xi_f(\beta X + \delta Y)\big]\,\big[(\alpha X + \gamma Y) + \xi_f'(\beta X + \delta Y)\big] \\ &= a\mathcal{N}(\beta\xi_f + \alpha)\Big[X + \frac{\delta\xi_f + \gamma}{\beta\xi_f + \alpha}Y\Big]\,\Big[X + \frac{\delta\xi_f' + \gamma}{\beta\xi_f' + \alpha}Y\Big] = a_1(X + \xi_1 Y)(X + \xi_1' Y)\,, \end{aligned}$$

where

$$\xi_f = \frac{b + \sqrt{\Delta}}{2a}\,, \quad a_1 = a\mathcal{N}(\beta\xi_f + \alpha) \quad \text{and} \quad \xi_1 = \frac{\delta\xi_f + \gamma}{\beta\xi_f + \alpha} = \begin{pmatrix} \delta & \gamma \\ \beta & \alpha \end{pmatrix} \xi_f\,.$$

This implies

$$\begin{aligned} 2a_1\xi_1 &= 2a\mathcal{N}(\beta\xi_f + \alpha)\,\frac{\delta\xi_f + \gamma}{\beta\xi_f + \alpha} = 2a(\delta\xi_f + \gamma)(\beta\xi_f' + \alpha) \\ &= 2a\big[\beta\delta\mathcal{N}(\xi_f) + \alpha\gamma + \alpha\delta\xi_f + \beta\gamma\xi_f'\big] \\ &= 2a\Big[\beta\delta\frac{c}{a} + \alpha\gamma + \alpha\delta\,\frac{b + \sqrt{\Delta}}{2a} + \beta\gamma\,\frac{b - \sqrt{\Delta}}{2a}\Big] \\ &= 2c\beta\delta + 2a\alpha\gamma + b(\alpha\delta + \beta\gamma) + (\alpha\delta - \beta\gamma)\sqrt{\Delta} \ = \ b_1 + \sqrt{\Delta}\,, \end{aligned}$$

and it follows that

$$\xi_1 = \frac{b_1 + \sqrt{\Delta}}{2a_1} = \xi_{Af}\,.$$

2. Let g be another non-degenerate form. If $g = Af$, then $d_g = d_f$, and $\xi_g = A^\dagger\xi_f$ by 1. To prove the converse, assume that $d_g = d_f$ and $\xi_g = A^\dagger\xi_f$. Then $g_1 = Af$ is a non-degenerate form, $\xi_{g_1} = A^\dagger\xi_f = \xi_g$ and $d_{g_1} = d_f = d_g$. Hence it follows that $g_1 = g$. □

Corollary 6.1.5. *Let f be a non-degenerate form of discriminant Δ. Then f is equivalent to f^- if and only if Pell's minus equation $x^2 - \Delta y^2 = -4$ has integral solutions.*

PROOF. Since $d_f = d_{f^-}$, Theorem 6.1.4 implies that f is equivalent to f^- if and only if ξ_f is equivalent to $\xi_{f^-} = -\xi_f$. By Theorem 1.3.8 this holds if and only if Pell's minus equation has integral solutions. □

Exercise 6.1.6. Let f be a non-degenerate form and $A \in \mathsf{GL}_2(\mathbb{Z}) \setminus \mathsf{SL}_2(\mathbb{Z})$. Prove that $\xi_{Af} = A^\dagger \xi_f'$.

If f is any non-degenerate form, then $d_f^{-1} f$ is a primitive non-degenerate form, and if f is negative definite, then $-f$ is positive definite. Therefore it is not really a loss of generality, and it often simplifies matters to restrict the investigations to not negative definite primitive forms. This motivates the following definition.

For a quadratic discriminant Δ, we denote by $\mathfrak{F}_\Delta$ the set of equivalence classes of not negative definite primitive forms of discriminant Δ. Explicitly,

$\mathfrak{F}_\Delta$ is the set of equivalence classes of

- positive definite primitive forms f of discriminant Δ if $\Delta < 0$,
- indefinite primitive forms f of discriminant Δ if $\Delta > 0$.

For a form $f = [a, b, c]$ of discriminant Δ, we denote by $[\![f]\!] = [\![a, b, c]\!] \in \mathfrak{F}_\Delta$ its equivalence class.

Theorem 6.1.7.

1. *Let Δ be a quadratic discriminant.*
   (a) *If $\Delta > 0$, then there is a bijective map $\vartheta_\Delta \colon \mathfrak{F}_\Delta \to \mathfrak{X}_\Delta^+$ onto the set $\mathfrak{X}_\Delta^+$ of proper equivalence classes of quadratic irrationals of discriminant Δ such that, for all primitive forms f of discriminant Δ,*
   $$\vartheta_\Delta([\![f]\!]) = [\xi_f]_{\sim^+} \quad \textit{(the proper equivalence class of } \xi_f).$$
   (b) *If $\Delta < 0$, then there is a bijective map $\vartheta_\Delta \colon \mathfrak{F}_\Delta \to \mathfrak{X}_\Delta$ onto the set $\mathfrak{X}_\Delta$ of equivalence classes of quadratic irrationals of discriminant Δ such that, for all positive definite primitive forms f of discriminant Δ,*
   $$\vartheta_\Delta([\![f]\!]) = [\xi_f]_{\sim} \quad \textit{(the equivalence class of } \xi_f).$$

   In both cases, it follows that
   $$|\mathfrak{F}_\Delta| = h_\Delta^+ .$$

2. *Regardless primitivity and definiteness, there are only finitely many equivalence classes of forms of discriminant Δ, and a complete set of representatives is obtained in the following way:*

   Suppose that $\Delta = \Delta_0 f_\Delta^2$, where Δ_0 is the fundamental discriminant and f_Δ is the conductor of Δ, and let $\{d_1, \ldots, d_k\}$ be the set of positive divisors of f_Δ. For $i \in [1, k]$, set $f_\Delta = d_i f_i$, let $\{\xi_{i,1}, \ldots, \xi_{i,l_i}\}$ be a complete set of representatives of proper equivalence classes of quadratic irrationals of discriminant $\Delta_0 f_i^2$, and suppose that $\xi_{i,j}$ is of type $(a_{i,j}, b_{i,j}, c_{i,j})$. Then
   $$\{[d_i a_{i,j}, d_i b_{i,j}, d_i c_{i,j}] \mid i \in [1, k], \ j \in [1, l_i]\}$$
   is a complete set of representatives of equivalence classes of forms of discriminant Δ.

Proof. 1. (a) Let $\Delta > 0$ be a quadratic discriminant. If f and g are primitive forms of discriminant Δ, then Theorem 6.1.4 implies that $f \sim g$ if and only if $[\xi_f]_{\sim_+} = [\xi_g]_{\sim_+}$. Hence there is an injective map $\vartheta_\Delta \colon \mathfrak{F}_\Delta \to \mathfrak{X}_\Delta^+$ such that $\vartheta(\llbracket f \rrbracket) = [\xi_f]_{\sim_+}$ for every primitive form f of discriminant Δ. On the other hand, for every quadratic irrational ξ of discriminant Δ, there exists a primitive form f of discriminant Δ such that $\xi_f = \xi$. Hence ϑ_Δ is surjective.

(b) Let $\Delta < 0$ be a quadratic discriminant. If f and g are positive definite primitive forms of discriminant Δ, then ξ_f and ξ_g both lie in the upper half-plane. Hence $\xi_f \sim \xi_g$ if and only if $\xi_f \sim_+ \xi_g$, and this holds if and only if $f \sim g$. Therefore there is an injective map $\vartheta_\Delta \colon \mathfrak{F}_\Delta \to \mathfrak{X}_\Delta$ such that $\vartheta(\llbracket f \rrbracket) = [\xi_f]_\sim$ for every positive definite primitive form f of discriminant Δ. On the other hand, if ξ is a quadratic irrational of discriminant Δ, then there is some $\varepsilon \in \{\pm 1\}$ such that $\varepsilon\xi$ lies in the upper half-plane, and there is a positive definite form f of discriminant Δ such that $\xi_f = \varepsilon\xi$. Since $\xi \sim -\xi$, it follows that $\vartheta(\llbracket f \rrbracket) = [\varepsilon\xi]_\sim = [\xi]_\sim$, and therefore ϑ_Δ is surjective. Finally, recall that in this case according to our definition we have $|\mathfrak{X}_\Delta| = h_\Delta = h_\Delta^+$

2. For $i \in [1, k]$ and $j \in [1, l_i]$, we set $f_{i,j} = [d_i a_{i,j}, d_i b_{i,j}, d_i c_{i,j}]$. Then $\Delta_{f_{i,j}} = \Delta$, $d_{f_{i,j}} = d_i$ and $\xi_{f_{i,j}} = \xi_{i,j}$. Hence the forms $f_{i,j}$ are pairwise not equivalent. If f is any form of discriminant Δ, then there is some $i \in [1, k]$ such that $d_f = d_i$, and since ξ_f is a quadratic irrational of discriminant $d_f^{-2}\Delta = \Delta_0 f_i^2$, there is some $j \in [1, l_i]$ such that $\xi_f \sim \xi_{i,j}$, and consequently $f \sim f_{i,j}$. □

Exercise 6.1.8. For any integer $\Delta \equiv 0 \text{ or } 1 \bmod 4$, derive a formula for the number h_Δ^* of all equivalence classes of forms of discriminant Δ in terms of various class numbers h_* (using the Theorems 6.1.7 and 6.1.3).

Let f be a non-degenerate form of discriminant Δ. A matrix $A \in \mathsf{SL}_2(\mathbb{Z})$ is called an *automorphism* of f if $Af = f$. As $(A, f) \mapsto Af$ is a group operation, it follows that the set $\mathsf{Aut}(f)$ of all automorphisms of f is a subgroup of $\mathsf{SL}_2(\mathbb{Z})$. Obviously, $\mathsf{Aut}(d_f^{-1} f) = \mathsf{Aut}(f)$.

For the next theorem recall the definition of $A^\dagger$ for a matrix $A \in \mathsf{SL}_2(\mathbb{Z})$ given before Theorem 6.1.4.

Theorem 6.1.9. *Let f be a non-degenerate form. Then there is a group isomorphism*

$$\mathsf{Aut}(f) \overset{\sim}{\to} \mathrm{Stab}^+(\xi_f)\,, \quad \textit{given by} \quad A \mapsto A^\dagger\,.$$

In particular, if f is a primitive form of discriminant Δ, the

$$|\mathsf{Aut}(f)| = \begin{cases} 2 & \textit{if} \quad \Delta < -4\,, \\ 4 & \textit{if} \quad \Delta = -4\,, \\ 6 & \textit{if} \quad \Delta = -3\,, \\ \infty & \textit{if} \quad \Delta > 0\,. \end{cases}$$

Proof. If $A \in \mathsf{SL}_2(\mathbb{Z})$, then Theorem 6.1.4 implies that $Af = f$ if and only if $A^\dagger \xi_f = \xi_f$. If f is a primitive form of discriminant Δ, then ξ_f is a quadratic irrational of discriminant Δ, and by Theorem 1.2.2 it follows that

$$|\mathsf{Aut}(f)| = |\mathrm{Stab}^+(\xi_f)| = |\{(x,y) \in \mathbb{Z}^2 \mid x^2 - \Delta y^2 = 4\}|\,. \qquad \square$$

Example 6.1.10. We calculate $\mathsf{Aut}(f)$ for the principal form $f = g_5 = [1,1,-1]$ of discriminant $\Delta_f = 5$. We have

$$\xi_f = \varepsilon_5 = \frac{1+\sqrt{5}}{2}\,, \quad \text{and} \quad \mathrm{Stab}^+(\varepsilon_5) = \left\{ \begin{pmatrix} \frac{x+y}{2} & y \\ y & \frac{x-y}{2} \end{pmatrix} \,\middle|\, x,\, y \in \mathbb{Z}\,,\ x^2 - 5y^2 = 4 \right\}$$

by Theorem 1.2.2. Hence Corollary 6.1.9 implies

$$\mathsf{Aut}(f) = \left\{ \begin{pmatrix} \frac{x-y}{2} & y \\ y & \frac{x+y}{2} \end{pmatrix} \,\middle|\, x,\, y \in \mathbb{Z}\,,\ x^2 - 5y^2 = 4 \right\}.$$

If $x,\, y \in \mathbb{Z}$, then it follows by the remarks after Theorem 5.2.1 that

$$x^2 - 5y^2 = 4 \quad \text{holds if and only if} \quad \frac{x + y\sqrt{5}}{2} \in \mathcal{O}_5^{\times +} = \langle -1, \varepsilon_5^2 \rangle\,,$$

and $\langle -1, \varepsilon_5^2 \rangle = \{\pm\varepsilon_5^{2m},\, \varepsilon_5'^{2m} \mid m \in \mathbb{N}_0\}$. By Example 5.9.10, we may calculate ε_5^{2m} for $m \in \mathbb{N}_0$ using the Fibonacci sequence and obtain $\varepsilon_5^{2m} = F_{2m+1} - F_{2m}\varepsilon_5'$, hence

$$\varepsilon_5^{2m} = \frac{u_m + v_m\sqrt{5}}{2}\,, \quad \text{where} \quad u_m = 2F_{2m+1} - F_{2m} \ \text{ and } \ v_m = F_{2m}\,.$$

Since

$$\begin{aligned} &\{(x,y) \in \mathbb{Z}^2 \mid x^2 - 5y^2 = 4\} \\ &\qquad = \{(u_m, v_m),\, (-u_m, v_m),\, (u_m, -v_m),\, (-u_m, -v_m) \mid m \in \mathbb{Z}\}\,, \end{aligned}$$

we obtain (with $F_{-1} = 0$)

$$\mathsf{Aut}(f) = \left\{ \pm\begin{pmatrix} F_{2m-1} & F_{2m} \\ F_{2m} & F_{2m+1} \end{pmatrix},\ \pm\begin{pmatrix} F_{2m+1} & -F_{2m} \\ -F_{2m} & F_{2m-1} \end{pmatrix} \,\middle|\, m \in \mathbb{N}_0 \right\},$$

Exercise 6.1.11. Calculate $\mathsf{Aut}(f)$ for the form $f = [1,0,-5]$ using the Fibonacci sequence.

6.2. Representation of integers

The following elementary Theorem 6.2.1 is basic for all assertions concerning the representation of integers by binary forms. It will be used again and again in the sequel, often without an explicit reference.

Theorem 6.2.1. *Let f be a form of discriminant Δ and $m \ne 0$ an integer.*

1. *f represents m if and only if there exists some $d \in \mathbb{N}$ such that $d^2 \mid m$ and f properly represents $d^{-2}m$. In particular, if m is squarefree and f represents m, then f properly represents m.*

2. *f properly represents m if and only if there exist integers $n,\, l \in \mathbb{Z}$ such that $f \sim [m,n,l]$, and then we can even achieve $n \in [b, b+2|m|-1]$ for an arbitrary integer $b \in \mathbb{Z}$.*
3. *If f is non-degenerate and represents 1, then f is equivalent to the principal form g_Δ.*
4. *If f is primitive and $M \in \mathbb{N}$ is any integer, then f properly represents some $m \in \mathbb{Z}$ such that $(M,m) = 1$, and $m \ge M$ unless f is negative definite.*

PROOF. 1. Suppose that f represents m, say $f(x,y) = m$, where $x,\, y \in \mathbb{Z}$, $(x,y) \ne (0,0)$, and set $d = (x,y)$. If $x = dx_1$ and $y = dy_1$, where $x_1,\, y_1 \in \mathbb{Z}$, then $(x_1,y_1) = 1$, and $d^{-2}m = f(x_1,y_1)$. Hence f properly represents $d^{-2}m$.

Conversely, if $d \in \mathbb{N}$, $d^2 \,|\, m$ and $x,\, y \in \mathbb{Z}$ are such that $f(x,y) = d^{-2}m$, then $f(dx,dy) = m$.

2. If $f \sim f_1 = [m,n,l]$ for some $n,\, l \in \mathbb{Z}$, then $f_1(1,0) = m$, hence f_1 and thus also f properly represents m.

Conversely, assume that f properly represents m, and let $\alpha, \beta \in \mathbb{Z}$ be such that $(\alpha,\beta) = 1$ and $m = f(\alpha,\beta)$. If $\gamma,\, \delta \in \mathbb{Z}$ are such that $\alpha\delta - \beta\gamma = 1$, then

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} f = [m,n',l'] \,, \quad \text{where} \quad n',\, l' \in \mathbb{Z}\,.$$

For every $b \in \mathbb{Z}$, there is some $k \in \mathbb{Z}$ is such that $n' + 2km \in [b, b+2|m|-1]$. Then we obtain

$$f \sim \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix} [m,n',l'] = [m,n,l]\,,$$

where $n = n' + 2km \in [b, b+2|m|-1]$ and $l \in \mathbb{Z}$.

3. If f is non-degenerate and represents 1, then $f \sim g = [1, \sigma, -D]$ for some $\sigma \in \{0,1\}$ and $D \in \mathbb{Z}^\bullet$. Since $\Delta = \sigma + 4D$, it follows that $g = g_\Delta$.

4. By Theorem 2.2.12, there exists a quadratic irrational ξ of type (m,b,c) such that ξ is properly equivalent to ξ_f, $(m,M) = 1$, and $m \ge M$ provided that $\xi_f \notin \mathfrak{H}^-$ (that is, f is not negative definite). Then f is equivalent to $[m,b,c]$ and thus properly represents m. □

Exercise 6.2.2. Let f be a form of discriminant Δ and m a squarefree divisor of Δ such that f (properly) represents m. Prove that there is some $c \in \mathbb{Z}$ such that $f \sim [m,0,c]$ or $f \sim [m,|m|,c]$.

Exercise 6.2.3. Let Δ be a quadratic discriminant, p a prime and f a form of discriminant Δ which represents p.

a) Prove that f is primitive if and only if $p \nmid f_\Delta$.

b) Let g be another form of discriminant Δ. Prove that g represents p if and only if g is improperly equivalent to f.

Theorem 6.2.4. *Let Δ be a quadratic discriminant, $m \ne 0$ an integer and m_0 the squarefree kernel of m.*

1. *m is properly represented by some form of discriminant Δ if and only if Δ is a quadratic residue modulo $4|m|$.*
2. *m is represented by some form of discriminant Δ if and only if m_0 is properly represented by some form of discriminant Δ.*

PROOF. 1. Let f be a form of discriminant Δ which properly represents m. Then it follows that $f \sim [m,n,l]$ for some $n,\ l \in \mathbb{Z}$, and $\Delta = n^2 - 4ml \equiv n^2 \mod 4|m|$.

As to the converse, let Δ be a quadratic residue modulo $4|m|$. Then there exist $n,\ l \in \mathbb{Z}$ such that $\Delta = n^2 - 4ml$, and $[m,n,l]$ is a form of discriminant Δ which properly represents m.

2. If m_0 is properly represented by some form of discriminant Δ, then obviously m is represented by the same form. Thus assume that m is represented by some form of discriminant Δ. Then it follows that $m = d^2 m_1$ for some $d \in \mathbb{N}$ and and an integer m_1 which is properly represented by the same form. Hence Δ is a quadratic residue modulo $4|m_1|$ by 1. and as $m_0 \mid m_1$, it follows that Δ is a quadratic residue modulo $4|m_0|$. Hence the assertion follows by 1. □

The shortcoming of Theorem 6.2.4 lies in the fact that it does not give criteria for the representation of an integer by a single form, but only by *some* (not necessarily primitive) form of a given discriminant. The representation by a single form is closely connected with the splitting behavior of primes in ring class fields, a topic which belongs to class field theory and is beyond the scope of this volume. We refer to [**82**] for an overview.

The "abelian part" of the theory of ring class fields can be described without using class field theory. This is done by Gauss' famous theory of genera, which we shall present in Section 6.4.

Nevertheless, there are special cases in which Theorem 6.2.4 yields criteria for the representation of integers by a single form. Let Δ be a quadratic discriminant such that $|\mathfrak{F}_\Delta| = 1$. Then every primitive form of discriminant Δ is equivalent to the principal form. Hence an integer m is (properly) represented by some primitive form f of discriminant Δ if and only if it is (properly) represented by the principal form. If, moreover, either $(\Delta, m) = 1$ or Δ is a fundamental discriminant, then every form which represents m is primitive. Among the examples for these special cases, there are many classical results found in the number-theoretic literature. We reformulate these special cases in the following corollary.

Corollary 6.2.5. *Let Δ be a quadratic discriminant such that $|\mathfrak{F}_\Delta| = 1$. Let f be a not negative definite primitive form of discriminant Δ, $m \in \mathbb{Z}$ and $m > 0$ if $\Delta < 0$. Suppose that either $(\Delta, m) = 1$ or that Δ is a fundamental discriminant.*

1. *m is properly represented by f if and only if Δ is a quadratic residue modulo $4|m|$.*
2. *m is represented by f if and only if Δ is a quadratic residue modulo $4m_0$, where m_0 is the squarefree kernel of m.*

PROOF. By assumption, every form f of discriminant Δ which properly represents m is primitive, and since $|\mathfrak{F}_\Delta| = 1$, every not negative definite primitive form of discriminant Δ is equivalent to the principal form. Hence m is properly represented by f if and only if it is properly represented by some form of discriminant Δ. Now the assertions follow by Theorem 6.2.4. $\square$

As a first application of our theory we give a fresh proof of Theorem 3.4.1 and supplement the Theorems 3.4.1 and 3.4.5. Quantitative refinements will be given in Theorem 6.2.13 and in Exercise 6.2.15.

Theorem 6.2.6 (Representations by the forms x^2+y^2 and $x^2\pm 2y^2$)**.**

1. *Let m be a positive integer.*
   - (a) *m is the sum of two coprime integral squares if and only if $4\nmid m$ and $p\nmid m$ for all primes $p\equiv 3 \bmod 4$.*
   - (b) *m is the sum of two integral squares if and only if $2\,|\,\mathsf{v}_p(m)$ for all primes $p\equiv 3 \bmod 4$.*
2. *Let m be an odd positive integer.*
   - (a) *There exist coprime integers $c,\,d\in\mathbb{Z}$ such that $m=c^2+2d^2$ if and only if all primes p dividing m satisfy $p\equiv 1$ or $3 \bmod 8$.*
   - (b) *There exist integers $c,\,d\in\mathbb{Z}$ such that $m=c^2+2d^2$ if and only if $2\,|\,\mathsf{v}_p(m)$ for all primes $p\equiv 5$ or $7 \bmod 8$.*
3. *For an odd integer m, the following assertions are equivalent:*
   - (a) *There exist integers $e,\,f\in\mathbb{Z}$ such that $m=e^2-2f^2$.*
   - (b) *There exist integers $s,\,t\in\mathbb{Z}$ such that $m=2s^2-t^2$.*
   - (c) *$2\,|\,\mathsf{v}_p(m)$ for all primes $p\equiv\pm 3 \bmod 8$..*
4. *Let $p\equiv 1 \bmod 8$ be a prime.*
   - (a) *Suppose that $p=8n+1=a^2+b^2=c^2+2d^2=e^2-2f^2=2s^2-t^2$ for some $a,\,b,\,c,\,d,\,e,\,f,\,s,\,t\in\mathbb{N}$ such that $4\,|\,b$. Then the following identities for Jacobi symbols hold:*

$$\Big(\frac{a}{p}\Big)=\Big(\frac{2b}{p}\Big)=\Big(\frac{f}{p}\Big)=\Big(\frac{d}{p}\Big)=1\,,\quad \Big(\frac{2}{a}\Big)=\Big(\frac{2}{t}\Big)=\Big(\frac{t}{p}\Big),$$

$$\Big(\frac{a+b}{p}\Big)=\Big(\frac{2}{a+b}\Big)=\Big(\frac{s}{p}\Big)=\Big(\frac{2}{t}\Big)(-1)^{b/4}=(-1)^{(s-1)/2}\,,$$

   and

$$\Big(\frac{c}{p}\Big)=\Big(\frac{e}{p}\Big)=\Big(\frac{2}{c}\Big)=\Big(\frac{-2}{e}\Big)=(-1)^{b/4}=(-1)^{n+d/2}\,.$$

   - (b) *If $p\equiv 9 \bmod 16$, then p is represented by exactly one of the forms $[1,0,32]$ and $[1,0,64]$. If $p\equiv 1 \bmod 16$, then p is represented either by both or by none of them.*

Proof. Throughout the proof, we shall use Corollary 6.2.5 and the properties of the Legendre and Jacobi symbols (see Chapter 3).

1. (a) m is the sum of two (coprime) integral squares if and only if m is (properly) represented by the form $g=g_{-4}=[1,0,1]$. Since -4 is a fundamental discriminant and $|\mathfrak{F}_{-4}|=h_{-4}=1$, it follows that m is properly represented by g if and only

if -4 is a quadratic residue modulo $4m$. Suppose that $m = 2^e m'$, where $e \in \mathbb{N}_0$, $m' \in \mathbb{N}$ and $2 \nmid m'$. Then -4 is a quadratic residue modulo $4m$ if and only if -4 is a quadratic residue modulo 2^{e+2} and modulo every odd prime dividing m. Since $-4 \equiv 2^2 \mod 8$, $x^2 \not\equiv -4 \mod 16$ for all $x \in \mathbb{Z}$ and

$$\Bigl(\frac{-4}{p}\Bigr) = \Bigl(\frac{-1}{p}\Bigr) = (-1)^{(p-1)/2} \quad \text{for every odd prime } p,$$

the assertion follows.

(b) Apply (a) to the squarefree kernel of m.

2. (a) $m = c^2 + 2d^2$ for some (coprime) integers $c,\, d \in \mathbb{Z}$ if and only if m is (properly) represented by the form $g = g_{-8} = [1,0,2]$. Since -8 is a fundamental discriminant and $|\mathfrak{F}_{-8}| = h_{-8} = 1$, it follows that m is properly represented by g if and only if -8 is a quadratic residue modulo $4m$, and as m is odd, this holds if and only if

$$\Bigl(\frac{-2}{p}\Bigr) = 1 \quad \text{and thus} \quad p \equiv 1 \text{ or } 3 \mod 8 \quad \text{for all primes dividing } m.$$

(b) Apply (a) to the squarefree kernel of m.

3. Let m be an odd integer. Then (a) holds if and only if m is represented by $[1,0,-2]$, and (b) holds if and only if m is represented by $[2,0,-1]$. Since $|\mathfrak{F}_8| = h_8^+ = 1$, the forms $[1,0,-2]$ and $[2,0,-1]$ are equivalent and represent the same integers. Since 8 is a fundamental discriminant, it follows that m is represented by these forms if and only if 8 is a quadratic residue modulo $4m_0$, where m_0 is the squarefree kernel of m. As m is odd, this holds if and only if

$$\Bigl(\frac{2}{p}\Bigr) = 1 \quad \text{and thus} \quad p \equiv \pm 1 \mod 8 \quad \text{for all primes } p \text{ dividing } m_0.$$

Since a prime p divides m_0 if and only if $2 \nmid \mathsf{v}_p(m)$, the latter condition holds if and only if $2 \,|\, \mathsf{v}_p(m)$ for all primes $p \equiv \pm 3 \mod 8$.

4. (a) By Theorem 3.4.5.1 we already know that

$$\Bigl(\frac{a}{p}\Bigr) = \Bigl(\frac{2b}{p}\Bigr) = 1\,, \quad \Bigl(\frac{a+b}{p}\Bigr) = \Bigl(\frac{2}{a+b}\Bigr) \quad \text{and} \quad 2^{(p-1)/4} \equiv (-1)^{b/4} \mod 2\,.$$

Since $p \equiv 1 \mod 8$, it follows that $s \equiv 1 \mod 2$, hence $2s^2 \equiv 2 \mod 16$ and therefore $p - 1 \equiv 1 - t^2 \mod 16$. It follows that

$$\frac{a^2-1}{8} = \frac{p-1}{8} - \frac{b^2}{8} \equiv \frac{p-1}{8} \equiv \frac{1-t^2}{8} \equiv \frac{t^2-1}{8} \mod 2$$

and

$$\frac{(a+b)^2-1}{8} \equiv \frac{p-1}{8} + \frac{ab}{4} \equiv \frac{t^2-1}{8} + \frac{b}{4} \mod 2\,,$$

hence

$$\Bigl(\frac{2}{a}\Bigr) = \Bigl(\frac{2}{t}\Bigr) \quad \text{and} \quad \Bigl(\frac{2}{a+b}\Bigr) = \Bigl(\frac{2}{t}\Bigr)(-1)^{b/4}\,.$$

Since $p = 2s^2 - t^2 \equiv 2s^2 \mod t$ and $p \equiv -t^2 \mod s$, we obtain

$$\Bigl(\frac{2}{t}\Bigr) = \Bigl(\frac{2s^2}{t}\Bigr) = \Bigl(\frac{p}{t}\Bigr) = \Bigl(\frac{t}{p}\Bigr), \quad (-1)^{(s-1)/2} = \Bigl(\frac{-1}{s}\Bigr) = \Bigl(\frac{-t^2}{s}\Bigr) = \Bigl(\frac{p}{s}\Bigr) = \Bigl(\frac{s}{p}\Bigr),$$

$$\Big(\frac{t}{p}\Big) \equiv (t^2)^{(p-1)/4} \equiv (2s^2)^{(p-1)/4} \equiv 2^{(p-1)/4}s^{(p-1)/2} \equiv (-1)^{b/4}\Big(\frac{s}{p}\Big) \mod p\,,$$

and therefore

$$\Big(\frac{s}{p}\Big) = (-1)^{b/4}\Big(\frac{t}{p}\Big) = (-1)^{b/4}\Big(\frac{2}{t}\Big)\,.$$

Suppose now that $d = 2^\delta d^*$ and $f = 2^\theta f^*$, where δ, θ, d^*, $f^* \in \mathbb{N}$ and $2 \nmid ced^*f^*$. Since $p \equiv 2d^2 \mod c$ and $p \equiv -2f^2 \mod e$, we obtain

$$\Big(\frac{c}{p}\Big) = \Big(\frac{p}{c}\Big) = \Big(\frac{2d^2}{c}\Big) = \Big(\frac{2}{c}\Big) \quad\text{and}\quad \Big(\frac{e}{p}\Big) = \Big(\frac{p}{e}\Big) = \Big(\frac{-2f^2}{e}\Big) = \Big(\frac{-2}{e}\Big)\,.$$

In the same way, $p \equiv c^2 \mod d^*$ and $p \equiv e^2 \mod f^*$ implies

$$\Big(\frac{d}{p}\Big) = \Big(\frac{d^*}{p}\Big) = \Big(\frac{p}{d^*}\Big) = 1 \quad\text{and}\quad \Big(\frac{f}{p}\Big) = \Big(\frac{f^*}{p}\Big) = \Big(\frac{p}{f^*}\Big) = 1\,.$$

Since $2d^2 \equiv -c^2 \mod p$, we obtain

$$\Big(\frac{2}{c}\Big) = \Big(\frac{c}{p}\Big) \equiv (-c^2)^{(p-1)/4} \equiv 2^{(p-1)/4}d^{(p-1)/2}(-1)^{b/4}\Big(\frac{d}{p}\Big) \equiv (-1)^{b/4} \mod p\,.$$

In the same way, $2f^2 \equiv e^2 \mod p$ implies

$$\Big(\frac{-2}{e}\Big) = \Big(\frac{e}{p}\Big) \equiv (e^2)^{(p-1)/4} \equiv 2^{(p-1)/4}f^{(p-1)/2} \equiv (-1)^{b/4}\Big(\frac{f}{p}\Big) \equiv (-1)^{b/4} \mod p\,,$$

and therefore

$$\Big(\frac{c}{p}\Big) = \Big(\frac{e}{p}\Big) = \Big(\frac{2}{c}\Big) = \Big(\frac{-2}{e}\Big) = (-1)^{b/4}\,.$$

On the other hand,

$$\frac{c^2-1}{8} = \frac{p-1}{8} - \frac{d^2}{4} \equiv n - \frac{d}{2} \mod 2\,, \quad\text{and}\quad \Big(\frac{2}{c}\Big) = (-1)^{(c^2-1)/8} = (-1)^{n-d/2}\,.$$

(b) We continue to use the notations of (a). Then p is represented by $[1,0,32]$ if and only if $p = c^2 + 2d^2$ for some integers c, d such that $d \equiv 0 \mod 4$, and p is represented by $[1,0,64]$ if and only if $p = a^2 + b^2$ for some integers a, b such that $b \equiv 0 \mod 8$. Hence the assertions follows since $(-1)^{b/4} = (-1)^{n+d/2}$, and therefore

$$n \equiv \frac{d}{2} + \frac{b}{4} \mod 2\,. \qquad \Box$$

Theorem 6.2.6.4(b) was only recently observed by I. Kaplansky [**60**]. A general theory concerning results of this type was given by D. Brink [**10**] using class field theory.

Exercise 6.2.7. Let $f = g_8 = [1,0,-2]$. Prove that

$$\mathsf{Aut}(f) = \left\{ \begin{pmatrix} u & y \\ 2y & u \end{pmatrix} \,\middle|\, u,\, y \in \mathbb{Z}\,,\ u^2 - 2y^2 = 1 \right\},$$

and show that every odd integer m properly represented by f has representations in the form $m = e^2 - 2f^2 = 2s^2 - t^2$, where e, f, s, $t \in \mathbb{N}$ and $e \equiv t \equiv 1 \mod 4$.

Exercise 6.2.8. Consider the forms $f = [1, 1, -1]$ and $g = [1, 0, -5]$. Prove that an integer m is properly represented by

- f if and only if all primes p dividing m satisfy $p \equiv \pm 1 \bmod 5$;
- g if and only if all odd primes p dividing m satisfy $p \equiv \pm 1 \bmod 5$, and either $2 \nmid m$ or $m \equiv 4 \bmod 8$.

Hint: 20 is a quadratic residue modulo $4|m|$ if and only if m is either represented by g or by $2f$.

Example 6.2.9. We consider the form $f = g_{12} = [1, 0, -3]$ of discriminant 12. Although $|\mathfrak{F}_{12}| = h_{12}^+ = 2$, it is possible to derive criteria for the representation of integers by f. Pell's minus equation $x^2 - 12y^2 = -4$ has no integral solutions, and therefore f and f^- are not equivalent (by Corollary 6.1.5). Since $f^- = [-1, 0, 3]$ is equivalent to $g = [3, 0, -1]$, it follows that every form of discriminant 12 is properly equivalent either to f or to g. By Theorem 6.2.4, an integer m is properly represented by either f or g if and only if 12 is a quadratic residue modulo $4|m|$, which holds if and only if 3 is a quadratic residue modulo $|m|$. By the elementary theory of quadratic residues, 3 is a quadratic residue modulo $|m|$ if and only if

$$9 \nmid m\,, \quad 4 \nmid m \quad \text{and} \quad \Big(\frac{3}{p}\Big) = 1 \quad \text{for all primes } p \neq 2,\, 3 \text{ dividing } m.$$

By Example 3.3.6.2, we obtain the following criterion:

> An integer m is properly represented by either f or g if and only if $9 \nmid m$, $4 \nmid m$, and all primes $p \neq 2$, 3 dividing m satisfy $p \equiv \pm 1 \bmod 12$.

Next we prove that an integer m cannot be properly represented by both f and g. Indeed, if $m = x^2 - 3y^2 = 3u^2 - v^2$, where $x,\ y,\ u,\ v \in \mathbb{Z}$ and $(x, y) = (u, v) = 1$, then $x^2 + u^2 = 3(y^2 + v^2)$, which contradicts Theorem 6.2.6.1(b). Now we can distinguish between f and g by the following simple congruence criterion.

Let m be an integer such that f is represented by either f or g.

- If $(m, 6) = 1$, then m is represented by f if and only if $m \equiv 1 \bmod 12$, and by g if and only if $m \equiv -1 \bmod 12$.
- If $3 \,|\, m$, then m is represented by f if and only if $m \equiv 3 \bmod 9$, and by g if and only if $m \equiv 6 \bmod 9$.
- If $2 \,|\, m$, then m is represented by f if and only if $m \equiv 0 \bmod 4$, and by g if and only if $m \equiv 2 \bmod 4$.

Later, in Section 6.3 we will see how genus theory can be used to derive criteria as above in a systematic way.

Exercise 6.2.10. Give necessary and sufficient conditions for an integer m to be of the form $m = x^2 - 6y^2$ for some $x,\ y \in \mathbb{Z}$ such that $(x, y) = 1$.

The following refinement of Theorem 6.2.1 paves the way for quantitative investigations of the representation of integers by forms.

Theorem 6.2.11. *Let f be a form of discriminant Δ and $m \neq 0$ an integer.*

1. *Let $x,\, y \in \mathbb{Z}$ be such that $(x,y)=1$ and $f(x,y)=m$. Then there exists a unique quadruple $(n,l,u,v) \in \mathbb{Z}^4$ such that $n \in [0, 2|m|-1]$, $xv-yu=1$, and*

$$\begin{pmatrix} x & y \\ u & v \end{pmatrix} f = [m,n,l]\,, \quad \text{hence} \quad \Delta = n^2 - 4ml.$$

2. *Suppose that*

$$\{n_1, \ldots, n_t\} = \{n \in [0, 2|m|-1] \mid n^2 \equiv \Delta \mod 4|m|\}\,.$$

For $j \in [1,t]$, let $l_j \in \mathbb{Z}$ be such that $n_j^2 - 4ml_j = \Delta$, set $g_j = [m, n_j, l_j]$, and let $J_f(m)$ be the set of all $j \in [1,t]$ such that $f \sim g_j$. If f properly represents m, then $J_f(m) \neq \emptyset$, and for each $j \in J_f(m)$, we fix integers x_j, y_j, u_j, v_j such that $x_jv_j - y_ju_j = 1$, and

$$\begin{pmatrix} x_j & y_j \\ u_j & v_j \end{pmatrix} f = g_j\,.$$

Then $(x_j, y_j) = 1$, $f(x_j, y_j) = m$, and there is a bijective map

$$\Theta \colon J_f(m) \times \mathsf{Aut}(f) \ \to \ \{(x,y) \in \mathbb{Z}^2 \mid (x,y)=1,\ f(x,y)=m\}$$

given by

$$\Theta(j,T) = (x,y) \quad \text{if and only if} \quad \begin{pmatrix} x_j & y_j \\ u_j & v_j \end{pmatrix} T = \begin{pmatrix} x & y \\ * & * \end{pmatrix}$$

for all $j \in J_f(m)$ and $T \in \mathsf{Aut}(f)$.

Proof. Suppose that $f = [a,b,c]$.

1. *Existence*: Since $(x,y)=1$, there exist u_1, $v_1 \in \mathbb{Z}$ such that $xv_1 - yu_1 = 1$, and there exists a unique $t \in \mathbb{Z}$ such that

$$n = 2axu_1 + b(xv_1 + yu_1) + 2cyv_1 + 2tm \ \in \ [0, 2\,|m|-1]\,.$$

Now we set $u = u_1 + tx$ and $v = v_1 + ty$. Then we get $xv - yu = 1$ and

$$\begin{pmatrix} x & y \\ u & v \end{pmatrix} f = [m,n,l]$$

for some $l \in \mathbb{Z}$.

Uniqueness: Suppose that (n,l,u,v), $(n',l',u',v') \in \mathbb{Z}^4$ are such that

$$xv - yu = xv' - yu' = 1\,, \quad \begin{pmatrix} x & y \\ u & v \end{pmatrix} = [m,n,l]\,, \quad \begin{pmatrix} x & y \\ u' & v' \end{pmatrix} = [m,n',l']\,,$$

and n, $n' \in [0, 2\,|m|-1]$. Then $x(v-v') = y(u-u')$, and since $(x,y)=1$, there is some $t \in \mathbb{Z}$ such that $u - u' = tx$. Therefore we obtain

$$n - n' = 2atx^2 + (bx + 2cy)(v-v') + btxy\,.$$

CASE 1: $x = 0$. Then it follows that $yu = yu' = -1$, hence $u = u'$, $y = \pm 1$, $t = 0$, $m = cy^2 = c$, $n - n' = 2my(v-v') \equiv 0 \mod 2|m|$, and therefore $n = n'$ and $v = v'$.

CASE 2: $x \neq 0$. Then we get $v - v' = ty$ and $n - n' = 2tm \equiv 0 \bmod 2|m|$. Again it follows that $n = n'$, $t = 0$, $v = v'$ and $u = u'$.

In both cases, we have $\Delta = n^2 - 4ml = n^2 - 4ml'$, and therefore $l = l'$.

2. Suppose that f properly represents m. Then we have $J_f(m) \neq \emptyset$ by 1., and if $j \in J_f(m)$, then

$$\begin{pmatrix} x_j & y_j \\ u_j & v_j \end{pmatrix} f = g_j \quad \text{for some matrix} \quad \begin{pmatrix} x_j & y_j \\ u_j & v_j \end{pmatrix} \in \mathsf{SL}_2(\mathbb{Z})\,.$$

In particular, it follows that $(x_j, y_j) = 1$ and $f(x_j, y_j) = m$. If $T \in \mathsf{Aut}(f)$ and

$$\begin{pmatrix} x_j & y_j \\ u_j & v_j \end{pmatrix} T = \begin{pmatrix} x & y \\ u & v \end{pmatrix}\,, \quad \text{then} \quad \begin{pmatrix} x & y \\ u & v \end{pmatrix} f = \begin{pmatrix} x_j & y_j \\ u_j & v_j \end{pmatrix} f = g_j = [m, n_j, l_j]\,,$$

which implies $(x, y) = 1$ and $f(x, y) = m$. Hence Θ is a well defined map.

Θ is surjective: Let $(x, y) \in \mathbb{Z}^2$ be such that $(x, y) = 1$ and $f(x, y) = m$. By 1., there exists a unique quadruple $(n, l, u, v) \in \mathbb{Z}^4$ such that $xv - yu = 1$, $n \in [0, 2|m| - 1]$ and

$$\begin{pmatrix} x & y \\ u & v \end{pmatrix} f = [m, n, l]\,.$$

By definition, there is some $j \in J_f(m)$ such that $n = n_j$, $l = l_j$,

$$\begin{pmatrix} x & y \\ u & v \end{pmatrix} f = g_j = \begin{pmatrix} x_j & y_j \\ u_j & v_j \end{pmatrix} f\,, \quad \text{hence} \quad T = \begin{pmatrix} x_j & y_j \\ u_j & v_j \end{pmatrix}^{-1} \begin{pmatrix} x & y \\ u & v \end{pmatrix} \in \mathsf{Aut}(f)\,,$$

and $(x, y) = \Theta(j, T)$.

Θ is injective: Suppose that $\Theta(i, T) = \Theta(j, T')$ for some i, $j \in J_f(m)$ and T, $T' \in \mathsf{Aut}(f)$, say

$$\begin{pmatrix} x_i & y_i \\ u_i & v_i \end{pmatrix} T = \begin{pmatrix} x & y \\ u & v \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} x_j & y_j \\ u_j & v_j \end{pmatrix} T' = \begin{pmatrix} x & y \\ u' & v'\,, \end{pmatrix}$$

where u, v, u', $v' \in \mathbb{Z}$ are such that $xv - yu = xv' - yu' = 1$. Then it follows that

$$\begin{pmatrix} x & y \\ u & v \end{pmatrix} f = \begin{pmatrix} x_i & y_i \\ u_i & v_i \end{pmatrix} = [m, n_i, l_i] \quad \text{and} \quad \begin{pmatrix} x & y \\ u' & v' \end{pmatrix} f = \begin{pmatrix} x_j & y_j \\ u_j & v_j \end{pmatrix} = [m, n_j, l_j]\,.$$

By the uniqueness in 1., we obtain $u = u'$, $v = v'$, $i = j$, and thus also $T = T'$. ☐

If a non-degenerate form of discriminant Δ represents some integer m, then Theorem 6.2.11 shows that there are infinitely many such representations if and only if $\Delta > 0$. In the next theorem, we give a precise formula for the number of representations of an integer by all forms of a given negative discriminant.

Theorem 6.2.12. *Let $\Delta < 0$ be a quadratic discriminant, $\{f_1, \ldots, f_h\}$ a complete set of representatives for the equivalence classes of positive definite forms with discriminant Δ, and*

$$w = \begin{cases} 2 & \text{if} \quad \Delta < -4\,, \\ 4 & \text{if} \quad \Delta = -4\,, \\ 6 & \text{if} \quad \Delta = -3\,. \end{cases}$$

For a positive integer m*, we set*

$$\Psi_\Delta(m) = \sum_{i=1}^{h} |\{(x,y)\in\mathbb{Z}^2 \mid (x,y)=1,\ f_i(x,y)=m\}|$$

and

$$\Psi^*_\Delta(m) = \sum_{i=1}^{h} |\{(x,y)\in\mathbb{Z}^2 \mid f_i(x,y)=m\}|\,.$$

1. *For every positive integer* m*, we have*

$$\Psi_\Delta(m) = w\,|\{n\in[0,2m-1] \mid n^2\equiv\Delta \mod 4m\}|\,.$$

2. *Assume that* $(\Delta,m)=1$*, let* m_0 *be the squarefree kernel of* m *and* r *the number of distinct primes dividing* m*. Then*

$$\Psi_\Delta(m) = w\sum_{d\,|\,m_0}\Bigl(\frac{\Delta}{d}\Bigr), \qquad \Psi^*_\Delta(m) = w\sum_{d\,|\,m}\Bigl(\frac{\Delta}{d}\Bigr),$$

and if $\Psi_\Delta(m)\ne 0$ *(which holds if and only if* Δ *is a quadratic residue modulo* $4m$*), then*

$$\Psi_\Delta(m) = 2^r w\,.$$

Proof. 1. Let $\{n_1,\ldots,n_t\}$ be the set of all integers $n\in[0,2m-1]$ satisfying $n^2\equiv\Delta \mod 4m$. For $j\in[1,t]$, let l_j be an integer such that $n_j^2-\Delta=4ml_j$, and set $g_j=[m,n_j,l_j]$. Then g_j is a positive definite form of discriminant Δ which properly represents m, and every positive definite form of discriminant Δ which properly represents m is equivalent to some g_j. For $i\in[1,h]$, it follows by Theorem 6.2.11.2 that

$$|\{(x,y)\in\mathbb{Z}^2 \mid (x,y)=1,\ f_i(x,y)=m\,\}| = |\mathsf{Aut}(f_i)|\,|\{j\in[1,t] \mid g_j\sim f_i\}|\,.$$

By Theorem 6.1.9 we obtain $|\mathsf{Aut}(f_i)|=w$ for all $i\in[1,h]$, and therefore

$$\begin{aligned}\Psi_\Delta(m) &= \sum_{j=1}^{t}\bigl|\{(x,y)\in\mathbb{Z}^2 \mid (x,y)=1,\ g_j(x,y)=m\,\}\bigr| = wt\\ &= w\,\bigl|\{n\in[0,2m-1] \mid n^2\equiv\Delta \mod 4m\}\bigr|\,.\end{aligned}$$

2. We maintain the notions of 1. and observe that

$$\{x+4m\mathbb{Z}\in\mathbb{Z}/4m\mathbb{Z} \mid x^2\equiv\Delta \mod 4m\} = \{\pm n_1,\ldots,\pm n_t\}\,.$$

By Theorem 3.5.11 we obtain

$$t = \bigl|\{n\in[0,2m-1] \mid n^2\equiv\Delta \mod 4m\}\bigr| = \sum_{d\,|\,m_0}\Bigl(\frac{\Delta}{d}\Bigr),$$

and if $t \ne 0$, then $t = 2^r$. This proves the formulas for $\Psi_\Delta(m)$, and it follows that

$$\Psi^*_\Delta(m) = \sum_{\substack{g\in\mathbb{N}\\ g^2\,|\,m}} \Psi_\Delta\Big(\frac{m}{g^2}\Big) = w \sum_{\substack{g\in\mathbb{N}\\ g^2\,|\,m}} \sum_{\substack{d_0\,|\,m_0\\ d_0g^2\,|\,m}} \Big(\frac{\Delta}{d_0}\Big) = w \sum_{d_0\,|\,m_0} \sum_{\substack{g\in\mathbb{N}\\ d_0g^2\,|\,m}} \Big(\frac{\Delta}{d_0g^2}\Big)$$

$$= w \sum_{d\,|\,m} \Big(\frac{\Delta}{d}\Big). \qquad \square$$

As a first application of Theorem 6.2.12 we consider again the representation of a positive integer as a sum of two squares.

Theorem 6.2.13. *Let m be a positive integer.*

1. *Assume that $4 \nmid m$ and $p \nmid m$ for all primes $p \equiv 3 \bmod 4$. Then*
$$|\{(x,y) \in \mathbb{Z}^2 \mid (x,y) = 1\,,\ m = x^2 + y^2\}| = 2^{r+2}\,,$$
where r is the number of distinct odd primes dividing m.
2. *If m is odd, then*
$$|\{(x,y) \in \mathbb{Z}^2 \mid m = x^2+y^2\}| = 4 \sum_{1\le d\,|\,m} (-1)^{(d-1)/2} = 4\,[\mathsf{d}_+(m) - \mathsf{d}_-(m)]\,,$$
where $\mathsf{d}_\pm(m)$ denotes the number of positive divisors $d \equiv \pm 1 \bmod 4$ of m.

Proof. If m is odd, then both assertions follow by Theorem 6.2.12.2.

It remains to prove 1. in the case $m = 2m_0$ for some odd $m_0 \in \mathbb{N}$. It suffices to prove that $|L| = |L_0|$, where $L = \{(x,y) \in \mathbb{Z}^2 \mid (x,y) = 1,\ x^2 + y^2 = m\}$ and $L_0 = \{(x,y) \in \mathbb{Z}^2 \mid (x,y) = 1,\ x^2+y^2 = m_0\}$. If $(x,y) \in L$, then $2 \nmid xy$,

$$\Big(\frac{x+y}{2}\Big)^2 + \Big(\frac{x-y}{2}\Big)^2 = m_0 \quad\text{and}\quad \Big(\frac{x+y}{2}, \frac{x-y}{2}\Big) = 1\,.$$

Indeed, if $d \in \mathbb{N}$, $2d \,|\, x+y$ and $2d \,|\, x-y$, then $2d \,|\, 2x$ and $2d \,|\, 2y$, hence $d \,|\, (x,y)$ and thus $d = 1$. Conversely, if $(x,y) \in L_0$, then $x + y \equiv 1 \bmod 2$,

$$(x+y)^2 + (x-y)^2 = m \quad\text{and}\quad (x+y, x-y) = 1\,.$$

Indeed, if $d \,|\, (x+y, x-y)$, then d is odd, $d \,|\, 2x$ and $d \,|\, 2y$, hence $d \,|\, (x,y)$ and thus $d = 1$.

Consequently, the maps $\Phi\colon L \to L_0$ and $\Phi_1\colon L_0 \to L$, defined by

$$\Phi(x,y) = \Big(\frac{x+y}{2}, \frac{x-y}{2}\Big) \quad\text{and}\quad \Phi_1(x,y) = (x+y, x-y)\,,$$

are mutually inverse bijections. $\square$

Recall from Theorem 3.4.2 that a positive integer m is said to have an essentially unique representation as a sum of two integral squares, if $m = a^2 + b^2 = c^2 + d^2$ (with a, b, c, $d \in \mathbb{Z}$) implies $\{|a|, |b|\} = \{|c|, |d|\}$.

Corollary 6.2.14. *A positive integer m has an essentially unique representation as a sum of two coprime integral squares if and only if $m = 2^\tau p^r$, where $\tau \in \{0,1\}$, $r \in \mathbb{N}_0$ and $p \equiv 1 \bmod 4$ is a prime.*

PROOF. We may assume that $m > 2$. By Theorem 3.4.1.1 it follows that m is the sum of two coprime integral squares if and only if $4 \nmid m$ and $p \nmid m$ for all primes $p \equiv 3 \bmod 4$, and m has an essentially unique representation as a sum of two coprime integral squares if and only if $|\{(x,y) \in \mathbb{Z}^2 \mid (x,y) = 1\,,\ m = x^2 + y^2\}| = 8$. Hence the assertion follows by Theorem 6.2.13.1. $\square$

Exercise 6.2.15. Let m be an odd positive integer. Prove that

$$\bigl|\{(x,y) \in \mathbb{Z}^2 \mid x^2 + 2y^2 = m\}\bigr| = 2\,[\mathsf{e}_1(m) - \mathsf{e}_3(m)]\,,$$

where, for $j \in \{1,3\}$, $\mathsf{e}_j(m)$ is the number of positive divisors $d \equiv \pm j \bmod 8$ of m. Calculate also $|\{(x,y) \in \mathbb{Z}^2 \mid (x,y) = 1,\ x^2 + 2y^2 = m\}|$.

Exercise 6.2.16. Let m be a positive integer such that $(m,6) = 1$, and let $\mathsf{e}_\pm(m)$ be the number of positive divisors $d \equiv \pm 1 \bmod 3$ of m. Prove that

$$\bigl|\{(x,y) \in \mathbb{Z}^2 \mid x^2 + 3y^2 = m\}\bigr| = 2\,[\mathsf{e}_+(m) - \mathsf{e}_-(m)]\,,$$

$$\bigl|\{(x,y) \in \mathbb{Z}^2 \mid x^2 + xy + y^2 = m\}\bigr| = 6\,[\mathsf{e}_+(m) - \mathsf{e}_-(m)]\,,$$

and deduce formulas for the numbers $|\{(x,y) \in \mathbb{Z}^2 \mid (x,y) = 1,\ x^2 + 3y^2 = m\}|$ and $|\{(x,y) \in \mathbb{Z}^2 \mid (x,y) = 1,\ x^2 + xy + y^2 = m\}|$.

6.3. Reduction

As for quadratic irrationals, we shall provide a procedure (called *reduction*) to determine distinguished representatives in each equivalence class of forms. As for quadratic irrationals, this is easy for negative discriminants. For positive discriminants we must go back to the theory of continued fractions.

Definition 6.3.1. Let Δ be a quadratic discriminant. A form f of discriminant Δ is called *reduced* if either

- $\Delta < 0$ and ξ_f is reduced, or
- $\Delta > 0$ and $|\xi_f|$ is reduced.

Since $\xi_f = \xi_{d_f^{-1}f}$, it follows that f is reduced if and only if the primitive form $d_f^{-1}f$ is reduced. Thus there is no loss of generality if we restrict to primitive forms in the sequel.

By definition, if $\Delta < 0$, then f is reduced if and only if $\xi_f \in \mathfrak{H}^+$, and then f is positive definite.

Theorem 6.3.2. *Let $\Delta < 0$ be a quadratic discriminant.*

1. *A positive definite (primitive) form $f = [a,b,c]$ of discriminant Δ is reduced if and only if either $-a < b \le a < c$ or $0 \le b \le a = c$, and then we have*

$$0 < a < \sqrt{\frac{|\Delta|}{3}} \quad \textit{and} \quad c > 0\,.$$

2. *Every class $F \in \mathfrak{F}_\Delta$ contains exactly one reduced form.*

Proof. 1. By Theorem 1.3.2.

2. Suppose that $F \in \mathfrak{F}_\Delta$ and $f \in F$. Then f is a positive definite primitive form, $\xi_f \in \mathfrak{H}^+$, and by Theorem 1.3.2.1 there exists a unique $\xi_0 \in \mathcal{F}$ such that $\xi_0 \sim_+ \xi_f$. Let f_0 be the unique primitive form such that $\xi_{f_0} = \xi_0$. Then f_0 is a positive definite primitive reduced form, $f_0 \sim f$ and thus $f_0 \in F$. If $f_1 \in F$ is any reduced form, then $\xi_{f_1} \sim \xi_{f_0}$, hence $\xi_{f_1} = \xi_{f_0}$ and therefore $f_1 = f_0$. □

Exercise 6.3.3. Prove that the following algorithm terminates after a finite number of steps and transforms a positive definite form into an equivalent reduced one.

```
 Input $a, b, c, \Delta$ with $a > 0$ and $\Delta = b^2 - 4ac < 0$.
Step 1. If either $c < a$, or if $c = a$ and $-a \le b < 0$, then set $a \leftarrow c$,
        $b \leftarrow -b$, $c \leftarrow a$, and go to Step 2.
Step 2. If $c \ge a$ and $|b| > a$, determine $k \in \mathbb{Z}$ such that $|b + 2ka| < a$,
        and set $b \leftarrow b + 2ka$, $c \leftarrow (b^2 - \Delta)/4a$, and go to Step 3.
Step 3. If $-a < b \le a < c$ or $0 \le b \le a = c$, output $a, b, c$ and
        terminate the algorithm. Otherwise go to Step 1.
```

Apply the algorithm to the form $[12, 14, 11]$.

Theorem 6.3.4. *Let $\Delta > 0$ be a quadratic discriminant, and let $f = [a, b, c]$ be a primitive form of discriminant Δ. Then the following assertions are equivalent*:

(a) *f is reduced.*

(b) $0 < \sqrt{\Delta} - b < 2|a| < \sqrt{\Delta} + b$.

(c) $0 < \sqrt{\Delta} - b < 2|c| < \sqrt{\Delta} + b$.

If these conditions are fulfilled, then $\{|a|,\, b,\, |c|\} \subset [1, \sqrt{\Delta}\,]$ *and* $ac < 0$.

Proof. 1. By definition, f is reduced if and only if either ξ_f or $-\xi_f$ is reduced. Since $-\xi_f$ is of type $(-a, b, -c)$, the assertion follows by Theorem 1.3.5. □

Now we go to describe a reduction algorithm for indefinite forms. We refer to Chapter 2 and in particular to Section 2.2 for the theory of continued fractions.

Remark and Definition 6.3.5. Let $\Delta > 0$ be a quadratic discriminant and $f = [a, b, c]$ a primitive form of discriminant Δ.

Let $\xi_f = [u_0, u_1, \ldots]$ be the continued fraction and $(\xi_n)_{n \ge 0}$ the sequence of complete quotients of ξ_f. Recall that the sequence $(\xi_n)_{n \ge 0}$ is recursively defined by $\xi_0 = \xi_f$ and $\xi_{n+1} = \xi_n^\#$ for all $n \ge 0$. If ξ_n is of type (a_n, b_n, c_n), then

$$\xi_n = \frac{b_n + \sqrt{\Delta}}{2a_n}\,, \quad u_n = \lfloor \xi_n \rfloor\,,$$

and we have the recursion formulas $a_0 = a$, $b_0 = b$, $a_{-1} = c_0 = c$,

$$b_{n+1} = -b_n + 2a_n u_n\,, \quad c_{n+1} = -a_n \quad \text{and} \quad a_{n+1} = \frac{\Delta - b_{n+1}^2}{4a_n} \quad \text{for all } n \ge 0\,.$$

For $n \ge 0$, we define

$$f_n = [(-1)^n a_n, b_n, (-1)^{n-1} a_{n-1}]\,.$$

Then f_n is a primitive form of discriminant Δ with root $\xi_{f_n} = (-1)^n \xi_n$. The formula

$$\xi_{f_{n+1}} = (-1)^{n+1}\xi_{n+1} = \frac{(-1)^{n+1}}{\xi_n - u_n} = \frac{(-1)^{n+1}}{(-1)^n \xi_{f_n} - u_n} = \begin{pmatrix} 0 & (-1)^{n+1} \\ (-1)^n & -u_n \end{pmatrix} \xi_{f_n}$$

shows that $\xi_{f_{n+1}}$ is properly equivalent to ξ_{f_n}. Hence it follows that $\xi_{f_n} \sim_+ \xi_f$ and thus $f_n \sim f$ for all $n \ge 0$.

Let now k be the pre-period length and λ the period length of the sequence $(\xi_n)_{n\ge 0}$. Recall that λ is odd if and only if Pell's minus equation $x^2 - \Delta y^2 = -4$ has integral solutions. We set

$$l = \begin{cases} \lambda & \text{if} \quad \lambda \equiv 0 \mod 2\,, \\ 2\lambda & \text{if} \quad \lambda \equiv 1 \mod 2\,. \end{cases}$$

By definition, k is the pre-period length and l is the period length of the sequence $((-1)^n \xi_n)_{n\ge 0}$ and thus of the sequence $(f_n)_{n\ge 0}$. In particular, it follows that $f_0, \ldots, f_{k+l-1}$ are distinct, and all forms in the period $(f_k, f_{k+1}, \ldots, f_{k+l-1})$ are reduced. We call $(f_k, f_{k+1}, \ldots, f_{k+l-1})$ the *period* of f.

Theorem 6.3.6. *Let $\Delta > 0$ be a quadratic discriminant.*

1. *Let f be a primitive form of discriminant Δ. Then the forms which occur in the period of f are reduced, and every reduced form which is equivalent to f occurs in the period.*
2. *Every class $F \in \mathfrak{F}_\Delta$ contains a reduced form $[a', b', c']$ such that $2\,|a'| < \sqrt{\Delta}$ and a reduced form $[a'', b'', c'']$ such that $a'' > 0$.*

Proof. We maintain all notions introduced in Remark and Definition 6.3.5.

1. We have already seen that all forms in the period $(f_k, f_{k+1}, \ldots, f_{k+l-1})$ of f are reduced. Let g be a reduced form equivalent to f. Then we have $\xi_g \sim_+ \xi_f$, and there is some $\sigma \in \{\pm 1\}$ such that $\sigma\xi_g$ is reduced. Since $(\xi_k, \xi_{k+1}, \ldots, \xi_\lambda)$ is the period of ξ_f, there exists some $j \in [k, k+l-1]$ such that $\varepsilon\xi_g = \xi_j = (-1)^j \xi_{f_j}$. If $\varepsilon = (-1)^j$, then $\xi_g = \xi_{f_j}$ and thus $g = f_j$. Assume now that $\varepsilon = (-1)^{j+1}$. Then it follows that $\xi_f \sim_+ \xi_g = (-1)^{j+1}\xi_j \sim_+ -\xi_f$, and by Theorem 1.3.8 there exist $x,\, y \in \mathbb{Z}$ such that $x^2 - \Delta y^2 = -4$. Hence λ is odd, $l = 2\lambda$, and

$$\xi_{f_{j+\lambda}} = (-1)^{j+\lambda}\xi_{j+\lambda} = (-1)^{j+\lambda}\xi_j = (-1)^{j+1}\xi_j = \xi_g\,.$$

2. Suppose that $F \in \mathfrak{F}_\Delta$, $f \in F$, and let $(f_n)_{n\ge 0}$ be the sequence defined in Remark and Definition 6.3.5. If $n \ge k$, then $f_n = [(-1)^n a_n, b_n, (-1)^{n-1} a_{n-1}]$ and $f_{n+1} = [(-1)^{n+1} a_{n+1}, b_{n+1}, (-1)^n a_n]$ are reduced forms, and Theorem 6.3.4 implies that $0 < b_{n+1} < \sqrt{\Delta}$. Hence we obtain $4|a_n a_{n+1}| = |\Delta - b_{n+1}^2| < \Delta$, hence either $2\,|a_n| < \sqrt{\Delta}$ or $2\,|a_{n+1}| < \sqrt{\Delta}$, and since

$$(-1)^n a_n (-1)^{n+1} a_{n+1} = -a_n a_{n+1} = c_{n+1} a_{n+1} < 0\,,$$

it follows that $(-1)^n a_n > 0$ or $(-1)^{n+1} a_{n+1} > 0$. □

Exercise 6.3.7. Calculate all periods of forms of discriminants 85 and 96.

Exercise 6.3.8. Write an algorithm for the following task:

Input: Two indefinite (not necessarily primitive) forms f and g.

Output: Decision whether or not f and g are equivalent and, if they are equivalent, a matrix $A \in \mathsf{SL}_2(\mathbb{Z})$ such that $g = Af$.

Apply the algorithm to the forms $f = [1, 0, -10]$ and $[-201, 244, -74]$.

6.4. Composition

Let Δ be a quadratic discriminant and (as in Section 6.1) $\mathfrak{F}_\Delta$ the set of all equivalence classes of not negative definite primitive forms of discriminant Δ. By Theorem 6.1.7, we have $|\mathfrak{F}_\Delta| = h_\Delta^+$.

Recall that for any form $f = [a, b, c]$ we denote by $[\![f]\!] = [\![a, b, c]\!] \in \mathfrak{F}_\Delta$ its equivalence class. For a class $F \in \mathfrak{F}_\Delta$, we simply write $F = [\![a, b, c]\!]$ to express that $f = [a, b, c]$ is a primitive not negative definite form and $F = [\![f]\!]$.

We have seen that equivalent forms (properly) represent the same integers. This observation motivates the following definition.

Definition 6.4.1. Let Δ be a quadratic discriminant, $F \in \mathfrak{F}_\Delta$ a class and m an integer. We say that F (properly) represents m if some (and then every) form $f \in F$ (properly) represents m. More generally, we say that a subset $\mathfrak{G} \subset \mathfrak{F}_\Delta$ (properly) represents m if some class $F \in \mathfrak{G}$ (properly) represents m.

A class $F \in \mathfrak{F}_\Delta$ properly represents an integer m if and only if $F = [\![m, b, c]\!]$ for some b, $c \in \mathbb{Z}$, and then F represents all numbers mt^2 for $t \in \mathbb{Z}$. If $M \in \mathbb{N}$, then Theorem 6.2.1.4 implies that every class $F \in \mathfrak{F}_\Delta$ is of the form $F = [\![a, b, c]\!]$, where $(a, M) = 1$ and $a \geq M$.

In this section we shall (following Gauss) define a group structure $*$ on $\mathfrak{F}_\Delta$ with the following property (see Corollary 6.4.8):

> If F_1, $F_2 \in \mathfrak{F}_\Delta$ and m_1, m_2 are integers such that F_1 represents m_1 and F_2 represents m_2, then $F_1 * F_2$ represents $m_1 m_2$.

Implicitly composition was first considered by L. L. Lagrange, but only Gauss observed that it gives rise to a group structure on $\mathfrak{F}_\Delta$. Although Gauss' definition is completely elementary (but by no means obvious), it is cumbersome to see that it really defines a group structure. More transparent approaches (though elementary as well) were given by A. M. Legendre and L. Dirichlet. A thorough historical discussion of the various concepts of composition is given in [**19**, §3].

We will embark on another strategy, essentially due to R. Dedekind. We shall establish a bijection between the set $\mathfrak{F}_\Delta$ and the narrow class group $\mathcal{C}_\Delta^+$ studied in Chapter 5. With the aid of this bijection we shall carry over the natural group structure of $\mathcal{C}_\Delta^+$ to $\mathfrak{F}_\Delta$.

A far-reaching generalization of these ideas was given by M. Bhargava. In a series of papers, he defined composition for forms of higher degree in several variables, connected with higher algebraic number fields (see [**8**] for a survey).

Theorem and Definition 6.4.2. *Let Δ be a quadratic discriminant.*

1. *There is a bijective map $\Phi_\Delta\colon \mathfrak{F}_\Delta \to \mathcal{C}_\Delta^+$ such that*
$$\Phi_\Delta(\llbracket f\rrbracket) = [I(\xi_f)]^+ = \Big[a, \frac{b+\sqrt{\Delta}}{2}\Big]^+ \in \mathcal{C}_\Delta^+$$
for every not negative definite primitive form $f=[a,b,c]$ of discriminant Δ with $a>0$.

   For F_1, $F_2 \in \mathfrak{F}_\Delta$, we define the *composition* $F_1 * F_2 \in \mathfrak{F}_\Delta$ such that Φ_Δ becomes a group isomorphism. Explicitly, we set
$$F_1 * F_2 = \Phi_\Delta^{-1}\big(\Phi_\Delta(F_1)\Phi_\Delta(F_2)\big)\,.$$
With this composition, $\mathfrak{F}_\Delta$ is an abelian group of order $|\mathfrak{F}_\Delta| = h_\Delta^+$ with unit element $H_\Delta = \llbracket g_\Delta\rrbracket$, and Φ_Δ is an isomorphism.

   The group $\mathfrak{F}_\Delta$ is called the *composition class group* or *form class group* of discriminant Δ. The class $H_\Delta = \llbracket g_\Delta\rrbracket$ of the principal form g_Δ is called the *principal class* of discriminant Δ.
2. *If $f=[a,b,c]$ is a primitive form of discriminant $\Delta>0$ such that $a<0$, then $\Phi_\Delta(\llbracket f\rrbracket) = [I(\xi_f)\sqrt{\Delta}]^+ \in \mathcal{C}_\Delta^+$.*
3. *Let $f=[a,b,c]$ be a not negative definite primitive form of discriminant Δ, and $f^{\mathsf{op}} = [a,-b,c]$. Then $\llbracket f\rrbracket * \llbracket f^{\mathsf{op}}\rrbracket = H_\Delta$ (and thus $\llbracket f^{\mathsf{op}}\rrbracket$ is the inverse of $\llbracket f\rrbracket$ in $\mathfrak{F}_\Delta$).* Consequently, if $F = \llbracket f\rrbracket$, we set $F^{-1} = \llbracket f^{\mathsf{op}}\rrbracket$.

PROOF. 1. Recall that $\mathfrak{X}_\Delta^{(+)}$ denotes the set of all (proper) equivalence classes of quadratic irrationals of discriminant Δ. By Theorem 6.1.7, there exist bijective maps
$$\vartheta_\Delta\colon \mathfrak{F}_\Delta \to \mathfrak{X}_\Delta \ \text{ if } \ \Delta<0, \quad \text{and} \quad \vartheta_\Delta\colon \mathfrak{F}_\Delta \to \mathfrak{X}_\Delta^+ \ \text{ if } \ \Delta>0,$$
and by Theorem 5.5.8 there exist bijective maps
$$\iota_\Delta\colon \mathfrak{X}_\Delta \to \mathcal{C}_\Delta = \mathcal{C}_\Delta^+ \ \text{ if } \ \Delta<0, \quad \text{and} \quad \iota_\Delta\colon \mathfrak{X}_\Delta^+ \to \mathcal{C}_\Delta^+ \ \text{ if } \ \Delta>0.$$
In any case,
$$\Phi_\Delta = \iota_\Delta\circ\vartheta_\Delta\colon \mathfrak{F}_\Delta \ \to \ \mathcal{C}_\Delta^+$$
is a bijective map. Explicitly, the maps ϑ_Δ and ι_Δ are given as follows:

CASE 1: $\Delta<0$. Then $\vartheta_\Delta(\llbracket f\rrbracket) = [\xi_f]_\sim$ (the equivalence class of ξ_f) for every positive definite primitive form of discriminant Δ, and $\iota_\Delta([\xi]_\sim) = [I(\xi)] = [I(\xi)]^+$ for every quadratic irrational ξ of discriminant Δ. Hence we get $\Phi_\Delta(\llbracket f\rrbracket) = [I(\xi_f)]^+$ for every positive definite primitive form of discriminant Δ (recall that a positive definite form $[a,b,c]$ has $a>0$).

CASE 2: $\Delta>0$. Then $\vartheta_\Delta(\llbracket f\rrbracket) = [\xi_f]_{\sim_+}$ (the proper equivalence class of ξ_f) for every indefinite primitive form of discriminant Δ, and $\iota_\Delta([\xi]_{\sim_+}) = [I(\xi)]^+$ for every quadratic irrational ξ of type (a,b,c) with $a>0$ and discriminant Δ. Hence we get $\Phi_\Delta(\llbracket f\rrbracket) = [I(\xi_f)]^+$ for every indefinite primitive form $[a,b,c]$ with $a>0$ of discriminant Δ (recall that, by Theorem 6.3.6.2, every class $F\in\mathfrak{F}_\Delta$ contains a form $[a,b,c]$ with $a>0$).

Since the basis number ω_Δ is the root of the principal form g_Δ, it follows that $\Phi(H_\Delta) = [I(\omega_\Delta)]^+ = [\mathcal{O}_\Delta]^+$, the unit element of $\mathcal{C}_\Delta^+$, and therefore H_Δ is the unit element of $\mathfrak{F}_\Delta$.

2. Let $f = [a, b, c]$ be a primitive form of discriminant $\Delta > 0$ such that $a < 0$. By Theorem 6.3.6.2 there exists a form $f' = [a', b', c']$ with $a' > 0$ such that $f' \sim f$ and thus $\xi_{f'} \sim_+ \xi_f$. Since $aa' < 0$, Theorem 5.5.7.1(b) yields

$$\Phi_\Delta(\llbracket f\rrbracket) = \Phi_\Delta(\llbracket f_1\rrbracket) = [I(\xi_{f_1})]^+ = [I(\xi_f)\sqrt{\Delta}\,]^+ \in \mathcal{C}_\Delta^+\,.$$

3. Since $\xi_{f^{\mathsf{op}}} = -\xi_f'$, it follows that $I(\xi_{f^{\mathsf{op}}}) = I(\xi_f') = I(\xi_f)'$. If $\operatorname{sgn}(a) = (-1)^\varepsilon$, where $\varepsilon \in \{0, 1\}$, then

$$\begin{aligned}\Phi_\Delta\big(\llbracket f\rrbracket * \llbracket f^{\mathsf{op}}\rrbracket\big) &= \Phi_\Delta\big(\llbracket f\rrbracket\big)\Phi_\Delta\big(\llbracket f^{\mathsf{op}}\rrbracket\big) = [I(\xi_f)(\sqrt{\Delta})^\varepsilon]^+\,[I(\xi_f)'(\sqrt{\Delta})^\varepsilon]^+ \\ &= [I(\xi_f)I(\xi_f)'\Delta^\varepsilon]^+ = [\mathfrak{N}_\Delta(I(\xi_f))\Delta^\varepsilon\mathcal{O}_\Delta]^+ = [\mathcal{O}_\Delta]^+ = \Phi_\Delta(H_\Delta)\,,\end{aligned}$$

and consequently $\llbracket f\rrbracket * \llbracket f^{\mathsf{op}}\rrbracket = H_\Delta$. □

Corollary 6.4.3. *Let Δ be a quadratic discriminant and $F \in \mathfrak{F}_\Delta$. Then F and F^{-1} (properly) represent the same integers.*

Proof. If $f \in F$, then f and f^{op} (properly) represent the same integers, and since $F^{-1} = \llbracket f^{\mathsf{op}}\rrbracket$, the assertion follows. □

Corollary 6.4.4. *Let $\Delta > 0$ be a quadratic discriminant and ε_Δ the fundamental unit of discriminant Δ. If $F = \llbracket a, b, c\rrbracket \in \mathfrak{F}_\Delta$ is the principal class, then*

$$|a| \ge \frac{u - e - 1}{v^2}\,, \quad \textit{where} \quad \varepsilon_\Delta = \frac{u + v\sqrt{\Delta}}{2} \quad \textit{and} \quad e = \mathcal{N}(\varepsilon_\Delta) \in \{\pm 1\}\,.$$

Proof. If F is the principal class, that

$$\Phi_\Delta(F) = [\mathcal{O}_\Delta]^+ = \begin{cases} [I(\xi_f)]^+ & \text{if} \quad a > 0\,, \\ [I(\xi_f)\sqrt{\Delta}\,]^+ & \text{if} \quad a < 0\,, \end{cases} \quad \text{where} \ \ I(\xi_f) = \Big[|a|, \frac{b + \sqrt{\Delta}}{2}\Big]\,.$$

In any case, $I(\xi_f) = \alpha\mathcal{O}_\Delta$ for some $\alpha \in \mathcal{O}_\Delta^\bullet$, and $|\mathcal{N}(\alpha)| = \mathfrak{N}_\Delta(I(\xi_f)) = |a|$. Hence the assertion follows by Theorem 5.2.9. □

In the following Theorem 6.4.5 we show how the classical formulas for composition follow from the ideal-theoretic definition given above. The basic idea in the classical definition is to define composition for special pairs of forms (called *concordant*), and to show that every pair of classes can be represented by a pair of concordant forms.

To be precise, two non-degenerate forms f_1, f_2 of the same discriminant are called *concordant* if there exist a_1, a_2, b, $c \in \mathbb{Z}$ such that

$$f_1 = [a_1, b, a_2c] \quad \text{and} \quad f_2 = [a_2, b, a_1c]\,.$$

In Theorem 6.4.5.2 we show that every pair of classes in $\mathfrak{F}_\Delta$ can be represented by a concordant pair of forms, and in Theorem 6.4.5.3 we give the formulas for the composition of concordant pairs.

Theorem 6.4.5. *Let* Δ *be a quadratic discriminant and* $F_1,\ F_2 \in \mathfrak{F}_\Delta$.

1. *For* $i \in \{1,2\}$, *suppose that* $F_i = \llbracket a_i, b_i, c_i \rrbracket$. *Then there exist* $B,\ C \in \mathbb{Z}$ *such that*
$$F_1 * F_2 = \left\llbracket \frac{a_1a_2}{e^2},\ B,\ C \right\rrbracket, \quad \textit{where} \quad e = \Bigl(a_1,\ a_2,\ \frac{b_1+b_2}{2}\Bigr).$$
2. *For every* $M \in \mathbb{N}$, *there exist integers* $a_1,\ a_2 \in \mathbb{N}$ *and* $b,\ c \in \mathbb{Z}$ *such that* $(a_1,a_2) = 1,\ \ (a_1a_2, M) = 1,\ \ F_1 = \llbracket a_1, b, a_2c \rrbracket$ *and* $F_2 = \llbracket a_2, b, a_1c \rrbracket$.
3. *Let* $a_1,\ a_2,\ b,\ c \in \mathbb{Z}$ *be such that* $F_1 = \llbracket a_1, b, a_2c \rrbracket$ *and* $F_2 = \llbracket a_2, b, a_1c \rrbracket$. *Then it follows that*
$$F_1 * F_2 = \llbracket a_1, b, a_2c \rrbracket * \llbracket a_2, b, a_1c \rrbracket = \llbracket a_1a_2, b, c \rrbracket\,,$$
and for all $x_1,\ x_2,\ y_1,\ y_2 \in \mathbb{Z}$, *we obtain*
$$(a_1x_1^2 + bx_1y_1 + a_2cy_1^2)(a_2x_2^2 + bx_2y_2 + a_1cy_2^2) = a_1a_2x^2 + bxy + cy^2,$$
where $x = x_1x_2 - cy_1y_2$ *and* $y = a_1x_1y_2 + a_2x_2y_1 + by_1y_2$.

Proof. For $i \in \{1,2\}$, Theorem 6.4.2.2 implies $\Phi_\Delta(F_i) = \llbracket \mathfrak{a}_i\sqrt{\Delta}^{\,\varepsilon_i} \rrbracket^+$, where
$$\mathfrak{a}_i = \Bigl[\,a_i, \frac{b_i+\sqrt{\Delta}}{2}\,\Bigr], \quad \varepsilon_i = \begin{cases} 0 & \text{if } a_i > 0\,, \\ 1 & \text{if } a_i < 0\,, \end{cases} \quad \text{and we set} \quad s = \frac{b_1+b_2}{2}\,.$$
By Theorem 5.4.6, we obtain $\mathfrak{a}_1\mathfrak{a}_2 = e\,\mathfrak{a}$, where
$$\mathfrak{a} = \Bigl[\,a, \frac{B+\sqrt{\Delta}}{2}\,\Bigr], \quad e = (a_1, a_2, s), \quad a = \frac{a_1a_2}{e^2}\,,$$
and if $u,\ v,\ w \in \mathbb{Z}$ are such that $e = a_1u + a_2v + sw$, then
$$B = b_2 + a_2v(b_1-b_2) - 2a_2wc_2\,.$$
$\mathfrak{a}$ is an $\mathcal{O}_\Delta$-regular ideal, $\operatorname{sgn}(a) = (-1)^{\varepsilon_1+\varepsilon_2}$, and there is some $C \in \mathbb{Z}$ such that $B^2 - 4aC = \Delta$ and $(a,B,C) = 1$. Now we obtain
$$\Phi_\Delta(F_1 * F_2) = [\mathfrak{a}_1\sqrt{\Delta}^{\,\varepsilon_1}]^+[\mathfrak{a}_2\sqrt{\Delta}^{\,\varepsilon_2}]^+ = [\mathfrak{a}\sqrt{\Delta}^{\,\varepsilon_1+\varepsilon}]^+ = \Phi_\Delta(\,\llbracket a, B, C \rrbracket) \in \mathcal{C}_\Delta^+\,,$$
and therefore $F_1 * F_2 = \llbracket a, B, C \rrbracket$, where $C \in \mathbb{Z}$ satisfies $B^2 - 4aC = \Delta$.

2. If $M \in \mathbb{N}$, then F_1 properly represents some $a_1 \in \mathbb{N}$ such that $(M, a_1) = 1$, and F_2 properly represents some $a_2 \in \mathbb{N}$ such that $(a_2, Ma_1) = 1$. Then it follows that $(a_1,a_2) = (M, a_1a_2) = 1$, $F_1 = \llbracket a_1, b_1, c_1 \rrbracket$ and $F_2 = \llbracket a_2, b_2, c_2 \rrbracket$ for some $b_1,\ c_1,\ b_2,\ c_2 \in \mathbb{Z}$. Since $\Delta = b_1^2 - 4a_1c_1 = b_2^2 - 4a_2c_2$, we obtain $b_1 \equiv b_2 \bmod 2$, and since $(2a_1, 2a_2) = 2 \mid b_1 - b_2$, there exist $l_1,\ l_2 \in \mathbb{Z}$ such that $2l_1a_1 - 2l_2a_2 = b_2 - b_1$. If $b = b_1 + 2l_1a_1 = b_2 + 2l_2a_2$, then it follows for $i \in \{1,2\}$ that
$$\begin{pmatrix} 1 & 0 \\ b_i & 1 \end{pmatrix} [a_i, b_i, c_i] = [a_i, b_i + 2l_ia_i, c_i'] = [a_i, b, c_i']\,,$$
where $c_i' \in \mathbb{Z}$ and $F_i = \llbracket a_i, b, c_i' \rrbracket$. Since $\Delta = b^2 - a_1c_1' = b^2 - a_2c_2'$, we get $a_1c_1' = a_2c_2'$. As $(a_1,a_2) = 1$, there is some $c \in \mathbb{Z}$ such that $c_2' = a_1c$, and consequently $c_1' = a_2c$, $F_1 = \llbracket a_1, b, a_2c \rrbracket$ and $F_2 = \llbracket a_2, b, a_1c \rrbracket$.

3. By assumption, we have $\Delta = b^2 - 4a_1a_2c$, and $(a_1, b, a_2c) = (a_2, b, a_1c) = 1$. We continue to use the notations of 1. and observe that $(a_1, a_2, b) \mid (a_1, b, a_2c)$. Hence we obtain $e = 1$, $a = a_1a_2$, $B = b - 2a_2wa_1c \equiv b \bmod 2a$, and therefore

$$\mathfrak{a} = \Big[a, \frac{b+\sqrt{\Delta}}{2} \Big], \quad \text{which implies} \quad F_1 * F_2 = [\![a_1a_2, b, C]\!], \quad \text{and} \quad C = \frac{b^2 - \Delta}{4a} = c\,.$$

The product formula is verified by a simple but lengthy calculation. □

Exercise 6.4.6. Let Δ be a quadratic discriminant, $F \in \mathfrak{F}_\Delta$, $\operatorname{ord}(F) \in \{1, 3\}$, and suppose that F represents some integers m and n. Prove that F represents mn as well.

Exercise 6.4.7.

a) Prove that an integer is (properly) represented by $f = [2, 4, 7]$ if and only if it is (properly) represented by $g = [2, 0, 5]$, and if two integers m and n are both represented by f or g, then there exist $x, y \in \mathbb{Z}$ such that $mn = x^2 + 10y^2$.

b) Prove that an integer is (properly) represented by $f = [3, 2, -3]$ if and only if it is (properly) represented by $g = [3, 4, -2]$, and if two integers m and n are both represented by f or g, then there exist $x, y \in \mathbb{Z}$ such that $mn = x^2 - 10y^2$.

Corollary 6.4.8. *Let Δ be a quadratic discriminant. Suppose that F_1, $F_2 \in \mathfrak{F}_\Delta$, and let m_1, m_2 be integers.*

1. *If F_1 represents m_1 and F_2 represents m_2, then $F_1 * F_2$ represents m_1m_2.*
2. *If F_1 properly represents m_1, F_2 properly represents m_2 and $(m_1, m_2) = 1$, then $F_1 * F_2$ properly represents m_1m_2.*

Proof. We apply Theorem 6.4.5.

1. There exist integers a_1, a_2, b, $c \in \mathbb{Z}$ such that $F_1 = [\![f_1]\!]$, $F_2 = [\![f_2]\!]$ and $F_1 * F_2 = [\![f]\!]$, where $f_1 = [a_1, b, a_2c]$, $f_2 = [a_2, b, a_1c]$ and $f = [a_1a_2, b, c]$. For $i \in \{1, 2\}$, let x_i, $y_i \in \mathbb{Z}$ be such that $f_i(x_i, y_i) = m_i$. Then $f(x, y) = m_1m_2$, where $x = x_1x_2 - cy_1y_2$ and $y = a_1x_1y_2 + a_2x_2y_1 + by_1y_2$. Hence $F_1 * F_2$ represents m_1m_2.

2. For $i \in \{1, 2\}$, suppose that F_i properly represents m_i. Then $F_i = [\![m_i, *, *]\!]$, and since $(m_1, m_2) = 1$, we obtain $F_1 * F_2 = [\![m_1m_2, *, *]\!]$. Hence $F_1 * F_2$ properly represents m_1m_2. □

Corollary 6.4.9. *Let Δ be a quadratic discriminant, and $F = [\![a, b, c]\!] \in \mathfrak{F}_\Delta$. Suppose that $a = a_1 \cdot \ldots \cdot a_n$, where $n \in \mathbb{N}$, $a_1, \ldots, a_n \in \mathbb{Z}$, and $a_1, \ldots, a_n \in \mathbb{N}$ if $\Delta < 0$. Suppose that either $(\Delta, a) = 1$, or $(a_i, a_j) = 1$ for all i, $j \in [1, n]$ such that $i \neq j$. Then it follows that $F_i = [\![\, a_i, b, a_1 \cdot \ldots \cdot a_{i-1}a_{i+1} \cdot \ldots \cdot a_nc \,]\!] \in \mathfrak{F}_\Delta$ for all $i \in [1, n]$, and $F = F_1 * \ldots * F_n$.*

Proof. We show first:

A. If $[1,n] = I' \uplus I''$ is a partition of $[1,n]$,

$$a' = \prod_{i\in I'} a_i \quad \text{and} \quad a'' = \prod_{i\in I''} a_i\,, \quad \text{then} \quad (a', b, a''c) = 1\,.$$

Proof of **A.** Assume to the contrary that $p\,|\,(a', b, a''c)$ for some prime p. Then $p\,|\,(a, b)$, hence $p\,|\,(\Delta, a)$, and therefore $(a_i, a_j) = 1$ for all $i,\, j \in [1,n]$ such that $i \ne j$. Consequently, $p\,|\,a'$ implies $p \nmid a''$ and thus $p\,|\,c$, a contradiction, since $(a, b, c) = 1$. $\square$[**A.**]

Now we proceed by induction on n. For $n = 1$, there is nothing to do.

$n \ge 2\,,\ n-1 \to n$: By **A**, and since $a_i > 0$ for all $i \in [1,n]$ if $\Delta < 0$, it follows that $F_i \in \mathfrak{F}_\Delta$ for all $i \in [1,n]$, and also that $F' = [\![\, a_1 \cdot \ldots \cdot a_{n-1}, b, a_n c]\!] \in \mathfrak{F}_\Delta$. By the induction hypothesis, we get $F' = F_1 * \ldots * F_{n-1}$, and by Theorem 6.4.5.3, we obtain $F = F' * F_n$. $\square$

Example 6.4.10. Let $a \ge 3$ be an odd integer, $n \in \mathbb{N}$, $\Delta = a^{2n} + 4$, and

$$F = \left[\!\!\left[\, a, a^{2n} - 2, \frac{a^{2n-1}(a^{2n}-5)}{4} \,\right]\!\!\right].$$

We assert that $\operatorname{ord}(F) \in \{n, 2n\}$, and for this, we shall prove that $F^{2n} = H_\Delta$ and $F^j \ne H_\Delta$ for all $j \in [1, n-1]$. For every $j \in \mathbb{N}$, Corollary 6.4.9 implies

$$F^j = \left[\!\!\left[\, a^j, a^{2n} - 2, \frac{a^{2n-j}(a^{2n}-5)}{4} \,\right]\!\!\right].$$

In particular, $F^{2n} = [\![f]\!]$, where

$$f = \left[a^{2n}, a^{2n} - 2, \frac{a^{2n}-5}{4} \right],$$

and as $f(1,-2) = -1$, it follows that $F^{2n} = H_\Delta$. By Corollary 5.2.6 we have

$$\varepsilon_\Delta = \frac{a^n + \sqrt{\Delta}}{2}\,, \quad \mathcal{N}(\varepsilon_\Delta) = -1\,.$$

Hence $F^j = H_\Delta$ implies $a^j \ge a^n$ (and therefore $j \le n$) by Corollary 6.4.4 (this construction is essentially due to P. Weinberger [**108**] and Y. Yamamoto [**112**]).

Theorem 6.4.11. *Let Δ be a quadratic discriminant and $F \in \mathfrak{F}_\Delta$. If there exists an integer m such that $(\Delta, m) = 1$ and F represents m^2, then it follows that $F \in \mathfrak{F}_\Delta^2$.*

PROOF. Let m be an integer such that $(\Delta, m) = 1$ and F represents m^2. Then there exists some $m_0 \in \mathbb{Z}$ such that $m_0\,|\,m$ and F properly represents m_0^2. Hence $F = [\![m_0^2, b, c]\!]$ for some $b,\, c \in \mathbb{Z}$ such that $\Delta = b^2 - 4m_0^2 c$. Since $(\Delta, m_0) = 1$, Corollary 6.4.9 (applied with $a_1 = a_2 = m_0$) implies $F = [\![m_0, b, m_0 c]\!]^2$. $\square$

Exercise 6.4.12. (Composition following Dirichlet) Let Δ be a quadratic discriminant. For $i \in \{1,2\}$, let $F_i = [\![a_i, b_i, c_i]\!] \in \mathfrak{F}_\Delta$, and $(a_1, a_2, \frac{1}{2}(b_1+b_2)) = 1$.

a) Prove that there is some $b \in \mathbb{Z}$ such that

$$b \equiv b_1 \mod 2a_1\,, \quad b \equiv b_2 \mod 2a_2 \quad \text{and} \quad b^2 \equiv \Delta \mod 4a_1a_2\,.$$

Hint: Prove that the conguences for b hold if and only if $a_2b \equiv a_2b_1 \mod 2a_1a_2$, $a_1b \equiv a_1b_2 \mod 2a_1a_2$ and $\frac{1}{2}(b_1+b_2)b \equiv \frac{1}{2}(b_1b_2+\Delta) \mod 2a_1a_2$.

b) Let b be as in **a)**. Prove that $F_1 * F_2 = [\![a_1a_2, b, c]\!]$, where $c \in \mathbb{Z}$ is such that $b^2 - \Delta = 4a_1a_2c$.

c) For $k \in \mathbb{N}$, consider the class $F_k = [\![2,1,k]\!] \in \mathfrak{F}_{1-4k}$. Prove that $\operatorname{ord}(F_k) \ge 5$ if $k \ge 9$, and calculate $\operatorname{ord}(F_k)$ for $k \in [1,8]$.

Theorem 6.4.13. *Let Δ be a quadratic discriminant.*

1. *Let m be a positive integer and $F \in \mathfrak{F}_\Delta$. Then F properly represents m if and only if there exists an $\mathcal{O}_\Delta$-regular ideal $\mathfrak{a} \in \Phi_\Delta(F)$ such that $m = \mathfrak{N}_\Delta(\mathfrak{a})$.*
2. *A prime p is represented by some class $F \in \mathfrak{F}_\Delta$ if and only if $p \nmid f_\Delta$ and $\mathsf{Q}_\Delta(p) \ne -1$ [equivalently, either $\mathsf{Q}_\Delta(p) = 1$, or $p \,|\, f_\Delta^{-2}\Delta$]. If this is the case, then F and F^{-1} are the only classes of $\mathfrak{F}_\Delta$ which represent p.*
3. *If $\Delta > 0$ and p is a prime, then $-p$ is represented by some class of $\mathfrak{F}_\Delta$ if and only if p is represented by some class of $\mathfrak{F}_\Delta$. If $F \in \mathfrak{F}_\Delta$ represents $-p$, then F and F^{-1} are the only classes of $\mathfrak{F}_\Delta$ which represent $-p$.*

Proof. 1. If F properly represents m, then $F = [\![m, b, c]\!]$ for some b, $c \in \mathbb{Z}$ such that $(m, b, c) = 1$, and then $\Phi_\Delta(F) = [\mathfrak{a}]^+ \in \mathcal{C}_\Delta^+$, where

$$\mathfrak{a} = \Big[m, \frac{b+\sqrt{\Delta}}{2}\Big] \quad \text{and} \quad \mathfrak{N}_\Delta(\mathfrak{a}) = m\,.$$

Conversely, let $\mathfrak{a} \in \Phi_\Delta(F)$ be an $\mathcal{O}_\Delta$-regular ideal such that $\mathfrak{N}_\Delta(\mathfrak{a}) = m$. Then $\mathfrak{a} = I(\xi)$, where ξ is a quadratic irrational ξ of type (m, b, c) (where b, $c \in \mathbb{Z}$) and discriminant Δ. Hence it follows that $\Phi_\Delta(F) = [\mathfrak{a}]_\Delta^+ = \Phi_\Delta([\![m, b, c]\!])$, and therefore $F = [\![m, b, c]\!]$ properly represents m.

2. We give an ideal-theoretic proof using the Theorems 5.8.1.3 and 5.8.8. An elementary proof using only binary forms can be deduced from Exercise 6.2.3.

Let p be a prime. Assume first that $F \in \mathfrak{F}_\Delta$ represents p. Then F properly represents p, and there exists an $\mathcal{O}_\Delta$-regular ideal $\mathfrak{p} \in \Phi_\Delta(F)$ such that $\mathfrak{N}_\Delta(\mathfrak{p}) = p$. It follows that $\mathfrak{p}$ is a prime ideal, $p \nmid f_\Delta$ and $\mathsf{Q}_\Delta(p) \ne -1$.

Conversely, suppose that $p \nmid f_\Delta$ and $\mathsf{Q}_\Delta(p) \ne -1$. Then there exists an $\mathcal{O}_\Delta$-regular prime ideal $\mathfrak{p}$ such that $\mathfrak{N}_\Delta(\mathfrak{p}) = p$, and then the class $F = \Phi^{-1}([\mathfrak{p}]^+)$ represents p. Since $\mathfrak{N}_\Delta(\mathfrak{p}) = \mathfrak{N}_\Delta(\mathfrak{p}') = p$ and $[\mathfrak{p}']^+ = ([\mathfrak{p}]^+)^{-1}$, it follows that also $\Phi_\Delta^{-1}([\mathfrak{p}']^+) = F^{-1}$ represents p. If $F_1 \in \mathfrak{F}_\Delta$ is any class which represents p, then (as we have proved) there exists an $\mathcal{O}_\Delta$-regular prime ideal $\mathfrak{p}_1 \subset \mathcal{O}_\Delta$ such that $\mathfrak{N}_\Delta(\mathfrak{p}_1) = p$ and $\Phi_\Delta(F_1) = [\mathfrak{p}_1]^+$. Since $\mathfrak{p}_1 \in \{\mathfrak{p}, \mathfrak{p}'\}$, it follows that $F_1 \in \{F, F^{-1}\}$.

3. For a class $F = [\![a, b, c]\!] \in \mathfrak{F}_\Delta$, we set $-F = [\![-a, -b, -c]\!] \in \mathfrak{F}_\Delta$. Then F represents $-p$ if and only if $-F$ represents p. If this is the case, then $-F$ and $(-F)^{-1}$ are the only classes of $\mathfrak{F}_\Delta$ which represent p, and therefore F and $-(-F)^{-1}$ are the only classes of $\mathfrak{F}_\Delta$ which represent $-p$. If $F = [\![a, b, c]\!]$, then

$(-F)^{-1} = [\![-a,-b,-c]\!]^{-1} = [\![-a,b,-c]\!] = -\,[\![a,-b,c]\!] = -F^{-1}$, and the assertion follows. $\square$

Let Δ be a quadratic discriminant and $d \in \mathbb{N}$. In Theorem 5.9.7, we established a group epimorphism $\Psi^+_{\Delta,d}\colon \mathcal{C}^+_{\Delta d^2} \to \mathcal{C}^+_\Delta$ such that $\Psi^+_{\Delta,d}([\mathfrak{a}]^+) = [\mathfrak{a}\mathcal{O}_\Delta]^+$ for every $\mathcal{O}_{\Delta d^2}$-regular ideal $\mathfrak{a}$ which is coprime to d. Using the terminology introduced in Theorem 6.4.2, we obtain an epimorphism $\Theta_{\Delta,d} = \Phi_\Delta^{-1} \circ \Psi^{(+)}_{\Delta,d} \circ \Phi_{\Delta d^2}\colon \mathfrak{F}_{\Delta d^2} \to \mathfrak{F}_\Delta$ which yields the commutative diagram

$$\begin{tikzcd}
\mathfrak{F}_{\Delta d^2} \arrow[r, "\Theta_{\Delta,d}"] \arrow[d, "\Phi_{\Delta d^2}"'] & \mathfrak{F}_\Delta \arrow[d, "\Phi_\Delta"] \\
\mathcal{C}^+_{\Delta d^2} \arrow[r, "\Psi^+_{\Delta,d}"] & \mathcal{C}^+_\Delta\,,
\end{tikzcd}$$

where the vertical arrows are isomorphisms. In the following Theorem 6.4.14 we give an explicit description of the epimorphism $\Theta_{\Delta,d}$.

Theorem 6.4.14. *Let Δ be a quadratic discriminant and $d \in \mathbb{N}$.*

1. *Every class $F \in \mathfrak{F}_{\Delta d^2}$ is of the form $F = [\![a, bd, cd^2]\!]$, where $a, b, c \in \mathbb{Z}$, $(a,b,c) = 1$, $(a, \Delta d) = 1$, $b \equiv \Delta \bmod 2$, and then $\Theta_{\Delta,d}(F) = [\![a,b,c]\!]$.*
2. *Suppose that $\Delta \equiv 1 \bmod 4$. Then the map $\Theta_{\Delta,2}\colon \mathfrak{F}_{4\Delta} \to \mathfrak{F}_\Delta$ is an isomorphism unless $\Delta \equiv 5 \bmod 8$ and either $\Delta < -3$, or $\Delta > 0$ and $\varepsilon_\Delta \in \mathcal{O}_{4\Delta}$. In this special case we have $|\mathrm{Ker}(\Theta_{\Delta,2})| = 3$ and*

$$\Big[\!\!\Big[\frac{1-\Delta}{4},\ \pm 2,\ 4\Big]\!\!\Big] \in \mathrm{Ker}(\Theta_{\Delta,2})\,.$$

Proof. 1. Suppose that $F \in \mathfrak{F}_{\Delta d^2}$, say $F = [\![a, b_1, c_1]\!]$, where $a,\, b_1,\, c_1 \in \mathbb{Z}$, $(a, b_1, c_1) = 1$, $(a, \Delta d) = 1$ and $b_1^2 - 4ac_1 = \Delta d^2$. Since $b_1 \equiv \Delta d \bmod 2$, there exist integers $u, l \in \mathbb{Z}$ such that $b_1 = \Delta d + 2u$, $la \equiv -u \bmod d$, and we obtain $b_1 + 2la \equiv b_1 - 2u \equiv \Delta d \bmod 2d$. Let $b \in \mathbb{Z}$ be such that $b_1 + 2la = bd$. Then $bd \equiv \Delta d \bmod 2d$, hence $b \equiv \Delta \bmod 2$, and

$$\begin{pmatrix} 1 & 0 \\ l & 1 \end{pmatrix} [a, b_1, c_1] = [a, bd, c_2] \quad \text{where} \quad c_2 \in \mathbb{Z} \quad \text{and} \quad 4ac_2 = (b^2 - \Delta)d^2\,.$$

Since $4 \,|\, b^2 - \Delta$ and $(a,d) = 1$, it follows that $d^2 \,|\, c_2$, and if $c_2 = cd^2$, where $c \in \mathbb{Z}$, then $F = [\![a, b_1, c_1]\!] = [\![a, bd, cd^2]\!]$ as asserted.

Since $(a,b,c) = 1$ and $\Delta = b^2 - 4ac$, it follows that $[\![a,b,c]\!] \in \mathfrak{F}_\Delta$. By Theorem 5.9.5.2, we obtain

$$\begin{aligned}\Phi_\Delta(\,[\![a,b,c]\!]) &= \Big[\,a,\ \frac{b+\sqrt{\Delta}}{2}\,\Big]^+ = \Psi^+_{\Delta,d}\Big(\Big[\,a,\ \frac{bd+\sqrt{\Delta d^2}}{2}\,\Big]^+\Big) \\ &= \Psi^+_{\Delta,d} \circ \Phi_{\Delta d^2}(\,[\![a, bd, cd^2]\!]) = \Phi_\Delta \circ \Theta_{\Delta,d}(\,[\![a, bd, cd^2]\!])\,,\end{aligned}$$

and therefore $[\![a,b,c]\!] = \Theta_{\Delta,d}(\,[\![a, bd, cd^2]\!])$.

2. By Corollary 5.9.9, $\Psi^+_{\Delta,2}$ (and consequently also $\Theta_{\Delta,2}$) is an isomorphism unless $\Delta \equiv 5 \bmod 8$ and $\mathcal{O}_\Delta^\times = \mathcal{O}_{4\Delta}^\times$. However, note that $\mathcal{O}_\Delta^\times = \mathcal{O}_{4\Delta}^\times$ if and only if either $\Delta < -3$, or $\Delta > 0$ and $\varepsilon_\Delta \in \mathcal{O}_{4\Delta}$.

If $\Delta \equiv 5 \bmod 8$ and $\mathcal{O}_\Delta^\times = \mathcal{O}_{4\Delta}^\times$, then $|\mathrm{Ker}(\Theta_{\Delta,2})| = |\mathrm{Ker}(\Psi_{\Delta,2}^+)| = 3$, and

$$\Big[\!\Big[\frac{1-\Delta}{4},\, \pm 2,\, 4\Big]\!\Big] = \Phi_{4\Delta}^{-1}\Big(\Big[\frac{1-\Delta}{4}, 1+\sqrt{\Delta}\Big]\Big) \in \mathrm{Ker}(\Theta_{\Delta,2})\,. \qquad \square$$

6.5. Theory of genera

This section, devoted to Gauss' genus theory, is the heart of the chapter on binary quadratic forms. If Δ is a quadratic discriminant and m is an integer, then we proved in Section 6.2 that m is represented by a class $F \in \mathfrak{F}_\Delta$ if and only if Δ is a quadratic residue modulo $4|m|$. However, we obtained no further information on the specific class F which represents m. By genus theory, we can determine at least the coset $F\mathfrak{F}_\Delta^2$. This is done by a system of quadratic characters associated with Δ, called *genus characters*, and the main tools for the proof are the theory of composition derived in the previous section and the theory of quadratic characters derived in Section 3.5.

We start with a series of definitions necessary for a lucid formulation of the main theorem (Theorem 6.5.3). Using this main theorem, we define genus characters and show their use for the representation of integers by binary forms. Only after that, we prove Gauss' duplication theorem (Theorem 6.5.11) which can be viewed as the crown of the theory. Gauss himself proved this theorem by means of ternary forms, and we shall reproduce his proof in the subsequent Section 6.6. In this section we present the proofs of P. G. L. Dirichlet and F. Mertens. Dirichlet's proof is very short, but uses the existence of primes in arithmetic progressions. Mertens' proof is ingenious and complicated but inside the theory of binary forms.

We recapitulate and amend a series of definitions and remarks from Chapter 3.

Let Δ be a quadratic discriminant and Δ^* the associated reduced discriminant, given in the form

$$\Delta = \mathrm{sgn}(\Delta)\, 2^e p_1^{e_1} \cdot \ldots \cdot p_r^{e_r} \quad \text{and} \quad \Delta^* = 2^{c(\Delta)} p_1 \cdot \ldots \cdot p_r\,,$$

where $e, r \in \mathbb{N}_0$, $e_1, \ldots, e_r \in \mathbb{N}$, $p_1, \ldots, p_r$ are distinct odd primes, and

$$c(\Delta) = \begin{cases} 0 & \text{if } \ \Delta \equiv 1 \bmod 4\,, \\ 1 & \text{if } \ \Delta \equiv 4 \bmod 16\,, \\ 2 & \text{if } \ \Delta \equiv 12 \bmod 16 \ \text{ or } \ \Delta \equiv 16 \bmod 32\,, \\ 3 & \text{if } \ \Delta \equiv 8 \bmod 16 \ \text{ or } \ \Delta \equiv 0 \bmod 32\,. \end{cases}$$

We consider the quadratic symbol $\mathsf{Q}_\Delta \colon \mathbb{Z} \to \{0, \pm 1\}$, defined for $a \in \mathbb{Z}$ by

$$\mathsf{Q}_\Delta(a) = \Big(\frac{\Delta}{a}\Big) \quad \text{if} \quad (\Delta, a) = 1\,, \quad \text{and} \quad \mathsf{Q}_\Delta(a) = 0 \quad \text{if} \quad (\Delta, a) \ne 1\,.$$

Recall that Q_Δ is a Dirichlet character modulo Δ^*, and we also view it as a quadratic character $\mathsf{Q}_\Delta \colon (\mathbb{Z}/\Delta^*\mathbb{Z})^\times \to \{\pm 1\}$ by means of $\mathsf{Q}_\Delta(a + \Delta^*\mathbb{Z}) = \mathsf{Q}_\Delta(a)$ for all $a \in \mathbb{Z}$ such that $(\Delta, a) = 1$. In particular, $\mathsf{Q}_\Delta \in \mathsf{X}(\Delta^*)$, and

$$\mathrm{Ker}(\mathsf{Q}_\Delta) = \{a + \Delta^*\mathbb{Z} \mid a \in \mathbb{Z},\ \mathsf{Q}_\Delta(a) = 1\} \subset (\mathbb{Z}/\Delta^*\mathbb{Z})^\times \ \text{ is a subgroup of index } 2\,.$$

We apply Theorem 3.5.10 to construct a basis of the group $\mathsf{X}(\Delta^*)[2]$ of all real characters modulo Δ^*. We recall the Gauss number, defined by

$$\mu(\Delta) = \begin{cases} r & \text{if} \quad \Delta \equiv 1 \mod 4 \ \text{ or } \ \Delta \equiv 4 \mod 16\,, \\ r+1 & \text{if} \quad \Delta \equiv 8 \text{ or } 12 \mod 16 \quad \text{or} \quad \Delta \equiv 16 \mod 32\,, \\ r+2 & \text{if} \quad \Delta \equiv 0 \mod 32\,. \end{cases}$$

In addition, we define the numbers

$$\eta(\Delta) = \begin{cases} 1 & \text{if} \quad \Delta \equiv 8 \mod 16\,, \\ 0 & \text{otherwise}\,, \end{cases} \qquad \text{and} \quad \rho(\Delta) = \begin{cases} r & \text{if} \quad c(\Delta) \le 1\,, \\ r+1 & \text{if} \quad c(\Delta) = 2\,, \\ r+2 & \text{if} \quad c(\Delta) = 3\,. \end{cases}$$

By these definitions, we obtain

$$\rho(\Delta) = \mu(\Delta) + \eta(\Delta\,.$$

Now we establish quadratic characters $\chi_1, \ldots, \chi_{\rho(\Delta)} \colon (\mathbb{Z}/\Delta^*\mathbb{Z})^\times \to \{\pm 1\}$. Note that for $m \in \mathbb{Z}$ we have $(\Delta, m) = 1$ if and only if $(m, \Delta^*) = 1$, and then the residue classes $m + p_i\mathbb{Z}$ for all $i \in [1, r]$ and $m + 2^{c(\Delta)}\mathbb{Z}$ are uniquely determined by the residue class $m + \Delta^*\mathbb{Z}$.

Suppose that $m \in \mathbb{Z}$ and $(\Delta, m) = 1$. We define

$$\chi_i(m + \Delta^*\mathbb{Z}) = \Bigl(\frac{m}{p_i}\Bigr) \quad \text{for } \ i \in [1, r].$$

If $c(\Delta) \ge 2$, we define $\chi_{r+1} = \varepsilon \colon (\mathbb{Z}/\Delta^*\mathbb{Z})^\times \to \{\pm 1\}$ by

$$\varepsilon(m + \Delta^*\mathbb{Z}) = \Bigl(\frac{-1}{m}\Bigr) = (-1)^{(m-1)/2} = \begin{cases} 1 & \text{if} \ \ m \equiv 1 \mod 4\,, \\ -1 & \text{if} \ \ m \equiv 3 \mod 4\,. \end{cases}$$

If $c(\Delta) \ge 3$, we define $\chi_{r+2} = \delta \colon (\mathbb{Z}/\Delta^*\mathbb{Z})^\times \to \{\pm 1\}$ by

$$\delta(m + \Delta^*\mathbb{Z}) = \Bigl(\frac{2}{m}\Bigr) = (-1)^{(m^2-1)/8} = \begin{cases} 1 & \text{if} \ \ m \equiv \pm 1 \mod 8\,, \\ -1 & \text{if} \ \ m \equiv \pm 3 \mod 8\,. \end{cases}$$

By Theorem 3.5.10, $(\chi_1, \ldots, \chi_{\rho(\Delta)})$ is a basis of $\mathsf{X}(\Delta^*)[2]$, and

$$|\mathsf{X}(\Delta^*)[2]| = ((\mathbb{Z}/\Delta^*\mathbb{Z})^\times \colon (\mathbb{Z}/\Delta^*\mathbb{Z})^{\times 2}) = 2^{\rho(\Delta)}\,.$$

Using this basis, we define the homomorphism

$$\boldsymbol{\varphi}_\Delta = (\varphi_1, \ldots, \varphi_{\mu(\Delta)}) \colon (\mathbb{Z}/\Delta^*\mathbb{Z})^\times \ \to \ \{\pm 1\}^{\mu(\Delta)}$$

by

$$\boldsymbol{\varphi}_\Delta = \begin{cases} (\chi_1, \ldots, \chi_r) & \text{if} \quad \Delta \equiv 1 \mod 4 \ \text{ or } \ \Delta \equiv 4 \mod 16\,, \\ (\chi_1, \ldots, \chi_r, \varepsilon) & \text{if} \quad \Delta \equiv 12 \mod 16 \ \text{ or } \ \Delta \equiv 16 \mod 32\,, \\ (\chi_1, \ldots, \chi_r, \delta) & \text{if} \quad \Delta \equiv 8 \mod 32\,, \\ (\chi_1, \ldots, \chi_r, \varepsilon\delta) & \text{if} \quad \Delta \equiv 24 \mod 32\,, \\ (\chi_1, \ldots, \chi_r, \varepsilon, \delta) & \text{if} \quad \Delta \equiv 0 \mod 32\,. \end{cases}$$

In particular, it follows that $\varphi_i = \chi_i$ for all $i \in [1,r]$, and if $c(\Delta) \geq 3$, $m \in \mathbb{Z}$ and $(\Delta, m) = 1$, then

$$\varepsilon\delta(m + \Delta^*\mathbb{Z}) = \Big(\frac{-2}{m}\Big) = (-1)^{(m^2-1/8+(m-1)/2} = \begin{cases} 1 & \text{if} \quad m \equiv 1 \text{ or } 3 \mod 8\,, \\ -1 & \text{if} \quad m \equiv 5 \text{ or } 7 \mod 8\,. \end{cases}$$

Now we make the crucial definitions for this section.

Definition 6.5.1. Let Δ be a quadratic discriminant.

1. The subgroup $\mathfrak{F}_\Delta^2 = \{F^2 \mid F \in \mathfrak{F}_\Delta\}$ of $\mathfrak{F}_\Delta$ is called the *principal genus*, the factor group $\mathfrak{F}_\Delta/\mathfrak{F}_\Delta^2$ is called the *genus group* and the elements χ of its character group $\widehat{\mathfrak{F}_\Delta/\mathfrak{F}_\Delta^2} = \widehat{\mathfrak{F}_\Delta}[2]$ are called *genus characters* of discriminant Δ. For a genus character χ and a class $F \in \mathfrak{F}_\Delta$, we set $\chi(F) = \chi(F\mathfrak{F}_\Delta^2)$ (based on the identification $\widehat{\mathfrak{F}_\Delta}[2] = \widehat{\mathfrak{F}_\Delta/\mathfrak{F}_\Delta^2}$, see Section A.7). For a class $F \in \mathfrak{F}_\Delta$, the coset $\mathsf{F} = F\mathfrak{F}_\Delta^2 \in \mathfrak{F}_\Delta/\mathfrak{F}_\Delta^2$ is called the *genus* of F, and if $f \in F$, then we call F the *genus of* f, and we say that f *lies in the genus* F.
2. For a class $F \in \mathfrak{F}_\Delta$, we denote by $\mathcal{H}_F$ the set of all prime residue classes $m + \Delta^*\mathbb{Z} \in (\mathbb{Z}/\Delta^*\mathbb{Z})^\times$ built by integers m such that $(\Delta, m) = 1$ and m is represented by F. Explicitly, we have
$$\mathcal{H}_F = \{f(x,y) + \Delta^*\mathbb{Z} \in (\mathbb{Z}/\Delta^*\mathbb{Z})^\times \mid f \in F,\ x,\, y \in \mathbb{Z},\ (\Delta, f(x,y) = 1)\}\,,$$
and we set $\mathcal{H}_\Delta = \mathcal{H}_{H_\Delta}$ (where $H_\Delta \in \mathfrak{F}_\Delta$ denotes the principal class). Explicitly, $\mathcal{H}_\Delta$ consists of all residue classes $m + \Delta^*\mathbb{Z} \in (\mathbb{Z}/\Delta^*\mathbb{Z})^\times$ built by integers $m \in \mathbb{Z}$ such that $(\Delta, m) = 1$ and $m = g_\Delta(x,y)$ for some x, $y \in \mathbb{Z}$.

Theorem 6.5.2. *Let Δ be a quadratic discriminant. Then*

$$|\mathfrak{F}_\Delta/\mathfrak{F}_\Delta^2| = 2^{\mu(\Delta)-1}\,.$$

Proof. By Theorem 6.4.2.1, there is an isomorphism $\Phi_\Delta \colon \mathfrak{F}_\Delta \xrightarrow{\sim} \mathcal{C}_\Delta^+$. It induces an isomorphism $\Phi_\Delta^* \colon \mathfrak{F}_\Delta/\mathfrak{F}_\Delta^2 \xrightarrow{\sim} \mathcal{C}_\Delta^+/\mathcal{C}_\Delta^{+2}$, and therefore (using Corollary A.5.5 and the Theorems 5.6.1 and 5.6.11) we obtain

$$|\mathfrak{F}_\Delta/\mathfrak{F}_\Delta^2| = |\mathcal{C}_\Delta^+/\mathcal{C}_\Delta^{+2}| = |\mathcal{C}_\Delta^+[2]| = |\mathcal{A}_\Delta^+| = 2^{\mu(\Delta)-1}\,. \qquad \square$$

The number $|\mathfrak{F}_\Delta/\mathfrak{F}_\Delta^2|$ is called the *genus number* of discriminant Δ.

Theorem 6.5.3 (Main theorem of genus theory)**.** *Let Δ be a quadratic discriminant.*

1. *The homomorphism $\boldsymbol{\varphi}_\Delta \colon (\mathbb{Z}/\Delta^*\mathbb{Z})^\times \to \{\pm 1\}^{\mu(\Delta)}$ is surjective,*
$$\mathcal{H}_\Delta = \operatorname{Ker}(\boldsymbol{\varphi}_\Delta) \supset (\mathbb{Z}/\Delta^*\mathbb{Z})^{\times 2}\,, \quad \big(\mathcal{H}_\Delta : (\mathbb{Z}/\Delta^*\mathbb{Z})^{\times 2}\big) = 2^{\eta(\Delta)}\,,$$
and $\boldsymbol{\varphi}_\Delta$ induces an isomorphism $\boldsymbol{\varphi}_\Delta^* \colon (\mathbb{Z}/\Delta^*\mathbb{Z})^\times/\mathcal{H}_\Delta \xrightarrow{\sim} \{\pm 1\}^{\mu(\Delta)}$.
2. *For all F, $G \in \mathfrak{F}_\Delta$, we have $\mathcal{H}_F\mathcal{H}_G \subset \mathcal{H}_{F*G}$.*

3. *If* $F \in \mathfrak{F}_\Delta$, $m \in \mathbb{Z}$, $(\Delta, m) = 1$ *and* F *represents* m, *then*
$$\mathcal{H}_F = (m + \Delta^*\mathbb{Z})\mathcal{H}_\Delta \subset \operatorname{Ker}(\mathsf{Q}_\Delta)\,.$$
In particular, $\mathcal{H}_F$ *is a coset of* $\mathcal{H}_\Delta$ *in* $\operatorname{Ker}(\mathsf{Q}_\Delta)$.
4. *The factor group* $\operatorname{Ker}(\mathsf{Q}_\Delta)/\mathcal{H}_\Delta$ *is an elementary* 2*-group, the map*
$$\Psi_\Delta \colon \mathfrak{F}_\Delta \to \operatorname{Ker}(\mathsf{Q}_\Delta)/\mathcal{H}_\Delta\,, \quad \textit{defined by} \quad \Psi_\Delta(F) = \mathcal{H}_F\,,$$
is a homomorphism, $\mathfrak{F}_\Delta^2 \subset \operatorname{Ker}(\Psi_\Delta)$,
$$|\operatorname{Ker}(\mathsf{Q}_\Delta)/\mathcal{H}_\Delta| = 2^{\mu(\Delta)-1} \quad \textit{and} \quad (\operatorname{Ker}(\Psi_\Delta)\colon\mathfrak{F}_\Delta^2) = (\operatorname{Ker}(\mathsf{Q}_\Delta)/\mathcal{H}_\Delta \colon \Psi_\Delta(\mathfrak{F}_\Delta))\,.$$

PROOF. We maintain all notations introduced at the beginning of this section.

1. By definition, $\boldsymbol{\varphi}_\Delta = (\varphi_1, \ldots, \varphi_{\mu(\Delta)}) \colon (\mathbb{Z}/\Delta^*\mathbb{Z})^\times \to \{\pm 1\}^{\mu(\Delta)}$ is a homomorphism, and $(\mathbb{Z}/\Delta^*\mathbb{Z})^{\times 2} \subset \operatorname{Ker}(\boldsymbol{\varphi}_\Delta)$. It suffices to prove the following assertions.

A. $\boldsymbol{\varphi}_\Delta$ is surjective, and $(\operatorname{Ker}(\boldsymbol{\varphi}_\Delta)\colon(\mathbb{Z}/\Delta^*\mathbb{Z})^{\times 2}) = 2^{\eta(\Delta)}$.

B. $(\mathbb{Z}/\Delta^*\mathbb{Z})^{\times 2} \subset \mathcal{H}_\Delta \subset \operatorname{Ker}(\boldsymbol{\varphi}_\Delta)$, and if $\Delta \equiv 8 \bmod 16$, then $\mathcal{H}_\Delta = \operatorname{Ker}(\boldsymbol{\varphi}_\Delta)$.

Suppose that **A** and **B** hold. If $\Delta \equiv 8 \bmod 16$, then $\mathcal{H}_\Delta = \operatorname{Ker}(\boldsymbol{\varphi}_\Delta)$ by **B**, and therefore $(\mathcal{H}_\Delta\colon(\mathbb{Z}/\Delta^*\mathbb{Z})^{\times 2}) = 2^{\eta(\Delta)}$ by **A**. If $\Delta \not\equiv 8 \bmod 16$, then $\eta(\Delta) = 0$, hence $\operatorname{Ker}(\varphi_\Delta) = \mathcal{H}_\Delta = (\mathbb{Z}/\Delta^*\mathbb{Z})^{\times 2}$, and therefore again $(\mathcal{H}_\Delta\colon(\mathbb{Z}/\Delta^*\mathbb{Z})^{\times 2}) = 1 = 2^{\eta(\Delta)}$. Obviously, $\boldsymbol{\varphi}_\Delta$ induces an isomorphism $\boldsymbol{\varphi}_\Delta^*$ as asserted.

Proof of **A**. To prove that $\boldsymbol{\varphi}_\Delta$ is surjective, let $\boldsymbol{e} = (e_1, \ldots, e_{\mu(\Delta)}) \in \{\pm 1\}^{\mu(\Delta)}$ be given. By the Chinese remainder theorem, there exists some $m \in \mathbb{Z}$ such that $(2\Delta, m) = 1$,
$$\Big(\frac{m}{p_i}\Big) = e_i \quad \text{for all} \quad i \in [1, r]\,,$$
and m has a preassigned value modulo 8. Since
$$(\varepsilon(m + \Delta^*\mathbb{Z}), \delta(m + \Delta^*\mathbb{Z})) = \begin{cases} (1,1) & \text{if} \quad m \equiv 1 \bmod 8\,, \\ (-1,-1) & \text{if} \quad m \equiv 3 \bmod 8\,, \\ (1,-1) & \text{if} \quad m \equiv 5 \bmod 8\,, \\ (-1,1) & \text{if} \quad m \equiv 7 \bmod 8\,, \end{cases}$$
it follows that $\boldsymbol{\varphi}$ is surjective. Now we obtain
$$\big(\operatorname{Ker}(\boldsymbol{\varphi}_\Delta)\colon(\mathbb{Z}/\Delta^*\mathbb{Z})^{\times 2}\big) = \frac{\big((\mathbb{Z}/\Delta^*\mathbb{Z})^\times \colon (\mathbb{Z}/\Delta^*\mathbb{Z})^{\times 2}\big)}{\big((\mathbb{Z}/\Delta^*\mathbb{Z})^\times \colon \operatorname{Ker}(\boldsymbol{\varphi}_\Delta)\big)} = \frac{2^{\rho(\Delta)}}{2^{\mu(\Delta)}} = 2^{\eta(\Delta)}\,. \quad \Box[\mathbf{A}.]$$

Proof of **B**. If $x \in \mathbb{Z}$ and $(\Delta, x) = 1$, then $x^2 = g_\Delta(x, 0)$. Hence the principal class $H_\Delta = [\![g_\Delta]\!]$ represents x^2. It follows that $(x + \Delta^*\mathbb{Z})^2 = x^2 + \Delta^*\mathbb{Z} \in \mathcal{H}_\Delta$, and therefore we must prove that

- $\mathcal{H}_\Delta \subset \operatorname{Ker}(\boldsymbol{\varphi}_\Delta)$, with equality if $\Delta \equiv 8 \bmod 16$, and
- $\mathcal{H}_\Delta \subset (\mathbb{Z}/\Delta^*\mathbb{Z})^{\times 2}$ if $\Delta \not\equiv 8 \bmod 16$ (as in this case $\operatorname{Ker}(\boldsymbol{\varphi}_\Delta) = \mathcal{H}_\Delta$ by **A**).

Suppose that $m \in \mathbb{Z}$, $(\Delta, m) = 1$, $m + \Delta^*\mathbb{Z} \in \mathcal{H}_\Delta$, and let x, $y \in \mathbb{Z}$ be such that $g_\Delta(x, y) \equiv m \bmod \Delta^*$.

CASE 1: $\Delta \equiv 1 \bmod 4$. If $u \in \mathbb{Z}$ is such that $2u \equiv 1 \bmod \Delta^*$, then

$$m \equiv 4u^2 g_\Delta(x,y) \equiv u^2\,[\,4x^2+4xy+(1-\Delta)y^2\,] \equiv [\,u(2x+y)\,]^2 \mod \Delta^*,$$

which implies $m+\Delta^*\mathbb{Z} \in (\mathbb{Z}/\Delta^*\mathbb{Z})^{\times 2}$.

CASE 2: $\Delta \equiv 0 \bmod 16$. Since $4\Delta^* \,|\, \Delta$, we obtain

$$m \equiv g_\Delta(x,y) \equiv x^2 - \frac{\Delta}{4}\,y^2 \equiv x^2 \mod \Delta^*,$$

which implies $m+\Delta^*\mathbb{Z} \in (\mathbb{Z}/\Delta^*\mathbb{Z})^{\times 2}$.

CASE 3: $\Delta \equiv 4 \bmod 16$. In this case, $\Delta^* = 2P$ and $\Delta = 4PP'$, where $P,\ P' \in \mathbb{Z}$ and $2 \nmid PP'$. Since $2 \nmid m$ and $m \equiv g_\Delta(x,y) \equiv x^2 - PP'y^2 \bmod 2P$, it follows that $x \not\equiv y \bmod 2$.

If $2\,|\,y$, then $m \equiv x^2 \bmod 2P$, and thus $m+\Delta^*\mathbb{Z} \in (\mathbb{Z}/\Delta^*\mathbb{Z})^{\times 2}$. If $2 \nmid y$, then $PP'y^2 \equiv -P^2 \bmod 2P$, hence $m \equiv x^2 - PP'y^2 \equiv x^2+P^2 \equiv (x+P)^2 \bmod 2P$, and thus again $m+\Delta^*\mathbb{Z} \in (\mathbb{Z}/\Delta^*\mathbb{Z})^{\times 2}$.

CASE 4: $\Delta \equiv 12 \bmod 16$. In this case, $\Delta^* = 4P$ and $\Delta = 4PP'$ for some $P,\ P' \in \mathbb{Z}$ such that $PP' \equiv 3 \bmod 4$. Since $m \equiv g_\Delta(x,y) \equiv x^2 - PP'y^2 \bmod 4P$ and $2 \nmid m$, it follows that $x \not\equiv y \bmod 2$.

If $2\,|\,y$, then $m \equiv x^2 \bmod 2P$. If $2 \nmid y$, then $P^2 + PP'y^2 \equiv 0 \bmod 4P$, and $m \equiv x^2 - PP'y^2 \equiv x^2+P^2 \equiv (x+P)^2 \bmod 4P$, since $2\,|\,x$. In both cases we obtain $m+\Delta^*\mathbb{Z} \in (\mathbb{Z}/\Delta^*\mathbb{Z})^{\times 2}$.

CASE 5: $\Delta \equiv 8 \bmod 16$. In this case, $\Delta^* = 8P$, where $P = p_1 \cdot \ldots \cdot p_r$, we set $\Delta = 4D$, where $D \in \mathbb{Z},\ D \equiv 2 \bmod 8$, and we observe that $g_\Delta = [1, 0-D]$.

a. $m+\Delta^*\mathbb{Z} \subset \mathrm{Ker}(\boldsymbol{\varphi}_\Delta)$: Since $m \equiv g_\Delta(x,y) \equiv x^2 - Dy^2 \bmod \Delta^*$, it follows that $m \equiv x^2 \bmod p_i$, hence $\varphi_i(m+\Delta^*\mathbb{Z}) = 1$ for all $i \in [1,r]$, and

$$m \equiv x^2 - Dy^2 \equiv \begin{cases} x^2-2y^2 \equiv \pm 1 \mod 8 & \text{if} \quad \Delta \equiv 8 \mod 32\,, \\ x^2+2y^2 \equiv 1 \text{ or } 3 \mod 8 & \text{if} \quad \Delta \equiv 24 \mod 32\,. \end{cases}$$

Hence $\delta(m+\Delta^*\mathbb{Z}) = 1$ if $\Delta \equiv 8 \bmod 32$, and $\varepsilon\delta(m+\Delta^*\mathbb{Z}) = 1$ if $\Delta \equiv 24 \bmod 32$. In both cases we obtain $m+\Delta^*\mathbb{Z} \in \mathrm{Ker}(\boldsymbol{\varphi}_\Delta)$.

b. $\mathrm{Ker}(\boldsymbol{\varphi}_\Delta) \subset \mathcal{H}_\Delta$: Suppose that $m \in \mathbb{Z},\ (\Delta,m)=1$ and $m+\Delta^*\mathbb{Z} \in \mathrm{Ker}(\boldsymbol{\varphi}_\Delta)$. Since $\varphi_i(m+\Delta^*\mathbb{Z}) = 1$ for all $i \in [1,r]$, it follows that m is a quadratic residue modulo P. Let $x_1 \in \mathbb{Z}$ be such that $m \equiv x_1^2 \bmod P$.

If $\Delta \equiv 8 \bmod 32$, then $m \equiv \pm 1 \bmod 8$, and there exist $x_2,\ y_2 \in \mathbb{Z}$ such that $m \equiv x_2^2 - 2y_2^2 \equiv x_2^2 - Dy_2^2 \bmod 8$. If $\Delta \equiv 24 \bmod 32$, then $m \equiv 1$ or $3 \bmod 8$, and there exist $x_2,\ y_2 \in \mathbb{Z}$ such that $m \equiv x_2^2 + 2y_2^2 \equiv x_2^2 - Dy_2^2 \bmod 8$. In both cases, let $x,\ y \in \mathbb{Z}$ be such that

$$x \equiv x_1 \mod P\,, \quad x \equiv x_2 \mod 8\,, \quad y \equiv 0 \mod P \quad \text{and} \quad y \equiv y_2 \mod 8\,.$$

Then it follows that $m \equiv x_1^2 \equiv x^2 - Dy^2 \bmod P$, $m \equiv x_2^2 - Dy_2^2 \equiv x^2 - Dy^2 \bmod 8$, hence $m \equiv x^2 - Dy^2 \bmod \Delta^*$, and therefore $m+\Delta^*\mathbb{Z} \in \mathcal{H}_\Delta$.

2. Suppose that $F,\ G \in \mathfrak{F}_\Delta$, and let $m,\ n \in \mathbb{Z}$ be such that $(\Delta,m) = (\Delta,n) = 1$, $m+\Delta^*\mathbb{Z} \in \mathcal{H}_F$, $n+\Delta^*\mathbb{Z} \in \mathcal{H}_G$, F represents m and G represents n. Then $F*G$ represents mn, and therefore $(m+\Delta^*Z)(n+\Delta^*\mathbb{Z}) = mn+\Delta^*\mathbb{Z} \in \mathcal{H}_{F*G}$.

3. Suppose that $F \in \mathfrak{F}_\Delta$, $m \in \mathbb{Z}$, $(\Delta, m) = 1$ and F represents m. By definition, we have $m + \Delta^*\mathbb{Z} \in \mathcal{H}_F$, and by 2. we obtain $(m + \Delta^*\mathbb{Z})\mathcal{H}_\Delta \subset \mathcal{H}_{F*H_\Delta} = \mathcal{H}_F$.

To prove the reverse inclusion, suppose that $n + \Delta^*\mathbb{Z} \in \mathcal{H}_F$, where $n \in \mathbb{Z}$, $(\Delta, n) = 1$, and F represents n. Then F^{-1} also represents n, and $H_\Delta = F * F^{-1}$ represents mn. Since $(\Delta, mn) = 1$, it follows that $mn + \Delta^*\mathbb{Z} \in \mathcal{H}_\Delta$, and therefore

$$\begin{aligned} n + \Delta^*\mathbb{Z} \in (n + \Delta^*\mathbb{Z})\mathcal{H}_\Delta &= (n + \Delta^*\mathbb{Z})(mn + \Delta^*\mathbb{Z})\mathcal{H}_\Delta \\ &= (m + \Delta^*\mathbb{Z})(n^2 + \Delta^*\mathbb{Z})\mathcal{H}_\Delta = (m + \Delta^*\mathbb{Z})\mathcal{H}_\Delta\,, \end{aligned}$$

since $n^2 + \Delta^*\mathbb{Z} \in (\mathbb{Z}/\Delta^*\mathbb{Z})^{\times 2} \subset \mathcal{H}_\Delta$ by 1.

It remains to prove that $m + \Delta^*\mathbb{Z} \in \operatorname{Ker}(\mathsf{Q}_\Delta)$. By assumption, m is represented by some form $f \in F$, and therefore $m = d^2 m_0$, where $d \in \mathbb{N}$ and $m_0 \in \mathbb{Z}$ is properly represented by f. Hence Δ is a quadratic residue modulo $4|m_0|$ by Theorem 6.2.4, and if $\Delta < 0$, then f is positive definite and therefore $m_0 > 0$. By Theorem 3.5.5.2, it follows that that $\mathsf{Q}_\Delta(m) = \mathsf{Q}_\Delta(m_0) = 1$, whence $m + \Delta^*\mathbb{Z} \in \operatorname{Ker}(\mathsf{Q}_\Delta)$.

4. Since $(\mathbb{Z}/\Delta^*\mathbb{Z})^{\times 2} \subset \mathcal{H}_\Delta \subset \operatorname{Ker}(\mathsf{Q}_\Delta) \subset (\mathbb{Z}/\Delta^*\mathbb{Z})^\times$, it follows that the factor group $\operatorname{Ker}(\mathsf{Q}_\Delta)/\mathcal{H}_\Delta$ is an elementary 2-group and, using 1.,

$$|\operatorname{Ker}(\mathsf{Q}_\Delta)/\mathcal{H}_\Delta| = \frac{\big((\mathbb{Z}/\Delta^*\mathbb{Z})^\times : (\mathbb{Z}/\Delta^*\mathbb{Z})^{\times 2}\big)}{\big((\mathbb{Z}/\Delta^*\mathbb{Z})^\times : \operatorname{Ker}(\mathsf{Q}_\Delta)\big)\big(\mathcal{H}_\Delta : (\mathbb{Z}/\Delta^*\mathbb{Z})^{\times 2}\big)} = \frac{2^{\rho(\Delta)}}{2^{1+\eta(\Delta)}} = 2^{\mu(\Delta)-1}\,.$$

If $F, G \in \mathfrak{F}_\Delta$, then $\Psi_\Delta(F * G) = \mathcal{H}_{F*G} \supset \mathcal{H}_F\mathcal{H}_G = \Psi_\Delta(F)\Psi_\Delta(G)$ by 2., and equality holds, since $\Psi_\Delta(F*G)$ and $\Psi_\Delta(F)\Psi_\Delta(G)$ are both cosets of $\mathcal{H}_\Delta$. Hence Ψ_Δ is a homomorphism, and since $\operatorname{Ker}(\mathsf{Q}_\Delta)/\mathcal{H}_\Delta$ is an elementary 2-group, we obtain $\mathfrak{F}_\Delta^2 \subset \operatorname{Ker}(\Psi_\Delta)$. Finally, we calculate

$$\begin{aligned} \big(\operatorname{Ker}(\mathsf{Q}_\Delta)/\mathcal{H}_\Delta : \Psi_\Delta(\mathfrak{F}_\Delta)\big) &= \frac{|\operatorname{Ker}(\mathsf{Q}_\Delta)/\mathcal{H}_\Delta|}{\big(\mathfrak{F}_\Delta : \operatorname{Ker}(\Psi_\Delta)\big)} = \frac{2^{\mu(\Delta)-1}\big(\operatorname{Ker}(\Psi_\Delta) : \mathfrak{F}_\Delta^2\big)}{(\mathfrak{F}_\Delta : \mathfrak{F}_\Delta^2)} \\ &= \big(\operatorname{Ker}(\Psi_\Delta) : \mathfrak{F}_\Delta^2\big)\,. \end{aligned}$$

□

Now we can define genus characters. Let Δ be a quadratic discriminant,

$$\boldsymbol{\varphi}_\Delta^* \colon (\mathbb{Z}/\Delta^*\mathbb{Z})^\times/\mathcal{H}_\Delta \xrightarrow{\sim} \{\pm 1\}^{\mu(\Delta)} \quad \text{and} \quad \Psi_\Delta \colon \mathfrak{F}_\Delta \to \operatorname{Ker}(\mathsf{Q}_\Delta)/\mathcal{H}_\Delta$$

as in Theorem 6.5.3, and define

$$\boldsymbol{\sigma}_\Delta = (\sigma_1, \ldots, \sigma_{\mu(\Delta)}) = \boldsymbol{\varphi}_\Delta^* \circ \Psi_\Delta \colon \mathfrak{F}_\Delta \to \{\pm 1\}^{\mu(\Delta)}\,.$$

Then $\boldsymbol{\sigma}_\Delta$ is a homomorphism, and the homomorphisms

$$\sigma_1, \ldots, \sigma_{\mu(\Delta)} \colon \mathfrak{F}_\Delta \to \{\pm 1\}$$

are called the *basic genus characters* associated with Δ. Since $\boldsymbol{\varphi}_\Delta^*$ is an isomorphism, it follows that $\operatorname{Ker}(\boldsymbol{\sigma}_\Delta) = \operatorname{Ker}(\Psi_\Delta) \supset \mathfrak{F}_\Delta^2$. Explicitly, $\boldsymbol{\sigma}_\Delta$ is given as follows:

If $F \in \mathfrak{F}_\Delta$, $m \in \mathbb{Z}$, $(\Delta, m) = 1$ and F represents m, then

$$\boldsymbol{\sigma}_\Delta(F) = \boldsymbol{\varphi}_\Delta(m + \Delta^*\mathbb{Z}) \in \{\pm 1\}^{\mu(\Delta)}\,.$$

If $F \in \mathfrak{F}_\Delta$, then the values $\sigma_j(F) \in \{\pm 1\}$ for $j \in [1, \mu(\Delta)]$ are called the *basic characters* of F, and the vector $\boldsymbol{\sigma}_\Delta(F) \in \{\pm 1\}^{\mu(\Delta)}$ is called the *complete character* of F. Since $\mathfrak{F}_\Delta^2 \subset \operatorname{Ker}(\boldsymbol{\sigma}_\Delta)$, the complete character $\boldsymbol{\sigma}_\Delta(F)$ only depends on the genus $F\mathfrak{F}_\Delta^2$ of F and not on the class itself. For a form $f \in F$, we set $\sigma_j(f) = \sigma_j(F)$ for all $j \in [1, \mu(\Delta)]$, and $\boldsymbol{\sigma}_\Delta(f) = \boldsymbol{\sigma}_\Delta(F)$.

Corollary 6.5.4. *Let Δ be a quadratic discriminant. Then every genus in $\mathfrak{F}_\Delta$ represents infinitely many primes.*

Proof. Let $\mathsf{F} = F\mathfrak{F}_\Delta^2 \in \mathfrak{F}_\Delta/\mathfrak{F}_\Delta^2$ be a genus, built by the class $F \in \mathfrak{F}_\Delta$. By Theorem 6.4.13.2, a prime p such that $(2\Delta, p) = 1$ is represented by some class of $\mathfrak{F}_\Delta$ if and only if $\mathsf{Q}_\Delta(p) = 1$, and (by the very definition of $\boldsymbol{\sigma}_\Delta$) it is represented by F if and only if $\boldsymbol{\sigma}_\Delta(F) = \boldsymbol{\varphi}_\Delta(p + \Delta^*\mathbb{Z})$. By Dirichlet's prime number theorem, every residue class in $(\mathbb{Z}/\Delta^*\mathbb{Z})^\times$ contains infinitely many primes, and thus the assertion follows. $\square$

Corollary 6.5.4 is a very weak assertion. In fact, even every class $F \in \mathfrak{F}_\Delta$ represents infinitely many primes. We shall prove this stronger assertion in Theorem 8.2.8 using the analytic theory of quadratic orders.

In the following Theorem 6.5.5 we show that for the calculation of the basic genus characters we need not revert to values coprime to the discriminant.

Theorem 6.5.5. *Let Δ be a quadratic discriminant and $F \in \mathfrak{F}_\Delta$. Then the complete character $\boldsymbol{\sigma}_\Delta(F) = (\sigma_1(F), \ldots, \sigma_{\mu(\Delta)}(F))$ can be calculated as follows.*

1. *If $j \in [1, r]$, $n \in \mathbb{Z} \setminus p_j\mathbb{Z}$ and F represents n, then*

$$\sigma_j(F) = \Big(\frac{n}{p_j}\Big).$$

2. *If $\Delta \equiv 0 \bmod 4$, $n \in \mathbb{Z} \setminus 2\mathbb{Z}$ and F represents n, then*

$$\sigma_{r+1}(F) = \begin{cases} (-1)^{(n-1)/2} & \text{if } \ \Delta \equiv 0 \text{ or } 12 \mod 16\,, \\ (-1)^{(n^2-1)/8} & \text{if } \ \Delta \equiv 8 \mod 32\,, \\ (-1)^{(n^2-1)/8+(n-1)/2} & \text{if } \ \Delta \equiv 24 \mod 32\,, \end{cases}$$

and

$$\sigma_{r+2}(F) = (-1)^{(n^2-1)/8} \quad \text{if} \quad \Delta \equiv 0 \mod 32\,.$$

Proof. Suppose that $m \in \mathbb{Z}$, $(\Delta, m) = 1$ and F represents m. Then

$$\sigma_j(F) = \varphi_j(m + \Delta^*\mathbb{Z}) \quad \text{for all} \quad j \in [1, \mu(\Delta)]\,.$$

1. Assume that $j \in [1, r]$, and let $n \in \mathbb{Z} \setminus p_j\mathbb{Z}$ be such that F represents n. Then it follows that $n = d^2 n_1$, where $d \in \mathbb{N}$, $n_1 \in \mathbb{Z}$, and F properly represents n_1. Consequently, $F = [\![n_1, b, c]\!]$ for some b, $c, \in \mathbb{Z}$, and there exist x, $y \in \mathbb{Z}$ such that $m = n_1x^2 + bxy + cy^2$. Since $\Delta = b^2 - 4n_1c$ and $4mn_1 = (2n_1x + by)^2 - \Delta y^2$, we obtain

$$1 = \Big(\frac{4mn_1}{p_j}\Big) = \Big(\frac{m}{p_j}\Big)\Big(\frac{n}{p_j}\Big), \quad \text{and therefore} \quad \sigma_j(F) = \Big(\frac{m}{p_j}\Big) = \Big(\frac{n}{p_j}\Big).$$

2. Suppose that $\Delta \equiv 0 \bmod 4$, $n \in \mathbb{Z} \setminus 2\mathbb{Z}$, and F represents n. As above, we get $n = d^2 n_1$, where $d \in \mathbb{N}$, $n_1 \in \mathbb{Z}$, F properly represents n_1, and $F = [\![n_1, 2b, c]\!]$ for some $b, c, \in \mathbb{Z}$. Since $2 \nmid d$, we have $n \equiv n_1 \bmod 8$. Let $x, y \in \mathbb{Z}$ be such that $m = n_1 x^2 + 2bxy + cy^2$. It follows that $\Delta = 4D$, where $D = b^2 - n_1 c$, and if $u = n_1 x + by$, then $mn_1 = u^2 - Dy^2 \equiv mn \bmod 8$.

If $\Delta \equiv 0$ or $12 \bmod 16$, then $D \equiv 0$ or $3 \bmod 4$, and $\sigma_{r+1}(F) = 1$ if and only if $m \equiv 1 \bmod 4$. Since $mn \equiv u^2$ or $u^2 + y^2 \bmod 4$ and $2 \nmid mn$, we get $mn \equiv 1 \bmod 4$, and therefore $\sigma_{r+1}(F) = (-1)^{(m-1)/2} = (-1)^{(n-1)/2}$.

If $\Delta \equiv 8 \bmod 32$, then $\sigma_{r+1}(F) = 1$ if and only if $m \equiv \pm 1 \bmod 8$, and since $mn = u^2 - Dy^2 \equiv u^2 - 2y^2 \equiv \pm 1 \bmod 8$, we obtain $n \equiv \pm 1 \bmod 8$ if and only if $m \equiv \pm 1 \bmod 8$, and therefore $\sigma_{r+1}(F) = (-1)^{(m^2-1)/8} = (-1)^{(n^2-1)/8}$.

If $\Delta \equiv 24 \bmod 32$, then $\sigma_{r+1}(F) = 1$ if and only if $m \equiv 1$ or $3 \bmod 8$. Since $mn = u^2 - Dy^2 \equiv u^2 + 2y^2 \equiv 1$ or $3 \bmod 8$, we obtain $n \equiv 1$ or $3 \bmod 8$ if and only if $m \equiv 1$ or $3 \bmod 8$. Hence $\sigma_{r+1}(F) = (-1)^{(m-1)/2 + (m^2-1)/8} = (-1)^{(n-1/2 + (n^2-1)/8}$.

If $\Delta \equiv 0 \bmod 32$, then $\sigma_{r+2}(F) = 1$ if and only if $m \equiv \pm 1 \bmod 8$, and since $mn \equiv u^2 \equiv 1 \bmod 8$, we obtain $n \equiv \pm 1 \bmod 8$ if and only if $m \equiv \pm 1 \bmod 8$. Hence $\sigma_{r+2}(F) = (-1)^{(m^2-1)/8} = (-1)^{(n^2-1)/8}$. □

Before we continue with our theory, we illustrate the use of genus characters by three examples.

Example 6.5.6 (Representation of integers by forms of discriminant -72)**.** We consider the discriminant $\Delta = -72 = -2^3 \cdot 3^2$. In this case, we have $\Delta^* = 24$ and $\mu(\Delta) = 2$.

An integer m is properly represented by some class $F \in \mathfrak{F}_{-72}$ if and only if $m > 0$ and -72 is a quadratic residue modulo $4m$. If $(6, m) = 1$, then this holds if and only if -2 is a quadratic residue modulo m, and thus if and only if all primes p dividing m satisfy $p \equiv 1$ or $3 \bmod 8$.

There are only 2 reduced forms of discriminant -72, namely

$$f_1 = g_{-72} = [1, 0, 18] \quad \text{and} \quad f_2 = [2, 0, 9]\,.$$

Hence $h_{-72} = 2$, and $\mathfrak{F}_{-72} = \{H, F_2\}$, where $H = H_{-72} = [\![f_1]\!]$ and $F_2 = [\![f_2]\!]$.

If a class $F \in \mathfrak{F}_{-72}$ represents some $m \in \mathbb{N}$ such that $(6, m) = 1$, then the complete character $\boldsymbol{\sigma}(F)$ is given by $\boldsymbol{\sigma}(F) = \boldsymbol{\sigma}_{-72}(F) = (\sigma_1(F), \sigma_2(F))$, where

$$\sigma_1(F) = \Big(\frac{m}{3}\Big), \quad \text{and} \quad \sigma_2(F) = (-1)^{(m-1)/2 + (m^2-1)/8} = \Big(\frac{-2}{m}\Big)\,.$$

By Theorem 6.5.5, $\sigma_1(F)$ can be calculated using any integer $m \in \mathbb{N} \setminus 3\mathbb{N}$. Obviously, H represents 1, and F_2 represents $11 = f_2(1,1)$. Hence it follows that $\boldsymbol{\sigma}(H) = (1,1)$, $\boldsymbol{\sigma}(F) = (-1,1)$, and we obtain the following criterion:

> If a positive integer $m \in \mathbb{N} \setminus 3\mathbb{N}$ is represented by some class class $F \in \mathfrak{F}_{-72}$, then m is represented by
>
> $$H \text{ if } m \equiv 1 \bmod 3\,, \quad \text{and by} \quad F_2 \text{ if } m \equiv 2 \bmod 3\,.$$

Example 6.5.7 (Representation of integers by forms of discriminant 60)**.** We consider the discriminant $\Delta = 60 = 2^2 \cdot 3 \cdot 5$. In this case, we have $\Delta^* = 60$ and $\mu(\Delta) = 3$.

An integer m is properly represented by some class $F \in \mathfrak{F}_{60}$ if and only if 60 is a quadratic residue modulo $4|m|$, and this holds if and only if 15 is a quadratic residue modulo $|m|$. Hence, if $(60, m) = 1$, then m is properly represented by some class $F \in \mathfrak{F}_{60}$ if and only if

$$\Big(\frac{15}{p}\Big) = 1 \quad \text{for all primes } p \text{ dividing } m\,.$$

By quadratic reciprocity,

$$\Big(\frac{15}{p}\Big) = \Big(\frac{3}{p}\Big)\Big(\frac{5}{p}\Big) = (-1)^{(p-1)/2}\Big(\frac{p}{3}\Big)\Big(\frac{p}{5}\Big) = 1$$

if and only if

$$\text{either } \ p \equiv 1 \bmod 4\,, \quad \Big(\frac{p}{3}\Big) = \Big(\frac{p}{5}\Big) \quad \text{or} \quad p \equiv -1 \bmod 4\,, \quad \Big(\frac{p}{3}\Big) = -\Big(\frac{p}{5}\Big)\,.$$

The following table gives the relevant residue classes of p.

p mod 4	p mod 3	p mod 5	p mod 60	$(\frac{p}{3})$	$(\frac{p}{5})$	$(\frac{-1}{p})$
1	1	±1	1, 49	1	1	1
1	-1	±2	17, 53	-1	-1	1
-1	1	±2	7, 43	1	-1	-1
-1	-1	±1	11, 59	-1	1	-1

Hence we obtain:

> An integer m such that $(60, m) = 1$ is properly represented by some form of discriminant 60 if and only if all primes p dividing m satisfy
>
> $$p \equiv 1,\ 7,\ 11,\ 17,\ 43,\ 49,\ 53 \ \text{ or } 59 \bmod 60\,.$$

To calculate $h_{60}^+ = |\mathfrak{F}_{60}|$, we determine all reduced forms of discriminant 60. By Theorem 6.3.4 a form $[a, b, c]$ (with $a,\ b,\ c \in \mathbb{Z}$, $(a, b, c) = 1$ and $60 = b^2 - 4ac$) is reduced if and only if $0 < \sqrt{60} - b < 2|a| < \sqrt{60} + b$, and as b is even, say $b = 2b_0$, this is equivalent to $0 < \sqrt{15} - b_0 < |a| < \sqrt{15} + b_0$. The solutions of these inequalities are

$$b_0 = 1,\ a \in \{3,\ 4\}\,, \quad b_0 = 2,\ a \in [2, 5] \quad \text{and} \quad b_0 = 3,\ a \in [1, 6]\,.$$

Since $b_0^2 - 15 = ac$, the only possible value is $b_0 = 3$, and the reduced forms of discriminant 60 are $[\pm1, 6, \mp6]$, $[\pm2, 6, \mp3]$, $[\pm3, 6, \mp2]$, $[\pm6, 6, \mp1]$. By Theorem 6.3.4 every class contains a form $[a, b, c]$ with $a > 0$. For $i \in [1, 4]$, we set $F_i = [\![f_i]\!]$, where

$$f_1 = [1, 6, -6], \quad f_2 = [2, 6, -3], \quad f_3 = [3, 6, -2] \quad \text{and} \quad f_4 = [6, 6, -1]\,.$$

Then $\mathfrak{F}_{60} = \{F_1,\ F_2,\ F_3,\ F_4\}$, and since $|\mathfrak{F}_{60}/\mathfrak{F}_{60}^2| = 2^{\mu(60)-1} = 4$, it follows that $|\mathfrak{F}_{60}| = 4$, $|\mathfrak{F}_{60}^2| = 1$, and every genus contains only one class.

If a class $F \in \mathfrak{F}_{60}$ represents an integer m such that $(60, m) = 1$, then the complete character $\boldsymbol{\sigma}(F)$ is given by

$$\boldsymbol{\sigma}(F) = \boldsymbol{\sigma}_{60}(F) = \Big(\big(\frac{m}{3}\big),\ \big(\frac{m}{5}\big),\ (-1)^{(m-1)/2}\Big)\,.$$

Since $f_1(1,0)=1$, $f_2(2,1)=17$, $f_3(1,2)=7$ and $f_4(0,1)=-1$, we obtain

$$\begin{aligned}
&\boldsymbol{\sigma}(F_1)=(1,1,1)\,, && \mathcal{H}_{F_1}=\{1+60\mathbb{Z},\,49+60\mathbb{Z}\,\} \quad \text{and} \quad F_1=H_{60}\,,\\
&\boldsymbol{\sigma}(F_2)=(-1,-1,1)\,, && \mathcal{H}_{F_2}=\{17+60\mathbb{Z},\,53+60\mathbb{Z}\,\}\,,\\
&\boldsymbol{\sigma}(F_3)=(1,-1,-1)\,, && \mathcal{H}_{F_3}=\{7+60\mathbb{Z},\,43+60\mathbb{Z}\,\}\,,\\
&\boldsymbol{\sigma}(F_4)=(-1,1,-1)\,, && \mathcal{H}_{F_4}=\{11+60\mathbb{Z},\,59+60\mathbb{Z}\,\}\,.
\end{aligned}$$

Therefore we obtain the following criterion:

> If an integer m such that $(60,m)=1$ is represented by some class $F\in\mathfrak{F}_{60}$, then m is represented by
>
> $$\begin{aligned} &F_1 \ \text{ if } \ m\equiv 1 \text{ or } 49 \bmod 60\,, && F_2 \ \text{ if } \ m\equiv 17 \text{ or } 53 \bmod 60\,,\\ &F_3 \ \text{ if } \ m\equiv 7 \text{ or } 43 \bmod 60\,, && F_4 \ \text{ if } \ m\equiv 11 \text{ or } 59 \bmod 60\,. \end{aligned}$$

In the examples 6.5.6 and 6.5.7 the class group $\mathfrak{F}_\Delta$ was in elementary 2-group. In this case, every genus consists of a single class, and therefore, using Theorem 6.5.3 (together with Theorem 6.5.5) we can completely determine the class representing a given integer by means of its character values.

If some genus F contains only one class C and its inverse C^{-1}, then an integer represented by F is represented by both C and C^{-1}, since C and C^{-1} represent the same integers (indeed, if $C=[\![f]\!]$, then $C^{-1}=[\![f^{\mathsf{op}}]\!]$, and obviously f and f^{op} represent the same integers). We illustrate this case by a further example.

Example 6.5.8 (Representation of integers by forms of discriminant -55)**.** We consider the discriminant $\Delta=-55=-5\cdot 11$. In this case, we have $\Delta^*=55$ and $\mu(\Delta)=2$.

An integer m is properly represented by some class $F\in\mathfrak{F}_{-55}$ if and only if $m>0$ and -55 is a quadratic residue modulo $4m$, and as $-55\equiv 1 \bmod 8$, this holds if and only if for all odd primes p dividing m we have

$$\Bigl(\frac{-55}{p}\Bigr)=\Bigl(\frac{5}{p}\Bigr)\Bigl(\frac{11}{p}\Bigr)=1\,, \quad \text{or, equivalently} \quad \Bigl(\frac{5}{p}\Bigr)=\Bigl(\frac{11}{p}\Bigr)\,.$$

There are only 4 reduced forms of discriminant -55, namely

$$f_1=g_{-55}=[1,1,14]\,, \quad f_2=[4,3,4]\,, \quad f_+=[2,1,7] \quad \text{and} \quad f_-=[2,-1,7]\,.$$

Hence we obtain $\mathfrak{F}_{-55}=\{H,F_2,F_+,F_-\}$, where $H=H_{-55}=[\![f_1]\!]$, $F_2=[\![f_2]\!]$, $F_\pm=[\![f_\pm]\!]$, and $|\mathfrak{F}_{-55}|=4$. Since $|\mathfrak{F}_{-55}/\mathfrak{F}_{-55}^2|=2$, it follows that $\mathfrak{F}_{-55}$ is a cyclic group of order 4, and since $F_-=F_+^{-1}\neq F_+$, we get $\mathfrak{F}_{-55}=\langle F_+\rangle$ and $F_+^2=F_2$. If a class $F\in\mathfrak{F}_{-55}$ represents some integer m such that $(55,m)=1$, then the complete character $\boldsymbol{\sigma}(F)=\boldsymbol{\sigma}_{-55}(F)=(\sigma_1(F),\sigma_2(F))$ is given by

$$\sigma_1(F)=\Bigl(\frac{m}{5}\Bigr) \quad \text{and} \quad \sigma_2(F)=\Bigl(\frac{m}{11}\Bigr)\,.$$

The classes of discriminant -55 fall into two genera, each containing two classes, namely $\mathsf{F}=\{H,F_2\}$ and $\mathsf{F}_1=\{F_+,F_-\}$. By definition, $\boldsymbol{\sigma}(H)=\boldsymbol{\sigma}(F_2)=(1,1)$, $\boldsymbol{\sigma}(F_\pm)=(-1,-1)$, and we obtain the following criterion:

If a positive integer m such that $(55, m) = 1$ is represented by some class $F \in \mathfrak{F}_{-55}$, then m is represented by

- either H of F_2 if $m \equiv \pm 1 \bmod 5$,
- both F_+ and F_- if $m \equiv \pm 2 \bmod 5$.

Exercise 6.5.9. Consider the discriminants $\Delta = -84$ and $\Delta = 96$. Determine all reduced forms of discriminant Δ, and establish necessary and sufficient congruence criteria for a positive integer m with $(\Delta, m) = 1$ to be represented by these forms.

Exercise 6.5.10. a) Let $q \equiv 1 \bmod 4$ be a prime such that $h_{-4q} = 2$ (there are only 3 such primes namely 5, 13 and 37, see [**100**]). Prove that every prime $p \neq q$ satisfying $p \equiv 1 \bmod 4$ and $\left(\frac{p}{q}\right) = 1$ is represented by $[1, 0, q]$.

b) Prove the following conjecture of Euler: If $p \neq 5$ is an odd prime, then p is represented by $[1, 0, 5]$ if and only if $p \equiv 1$ or $9 \bmod 20$, and $2p$ is represented by $[1, 0, 5]$ if and only if $p \equiv 3$ or $7 \bmod 20$.

Although we already gave several non-trivial applications, the results proved hitherto are incomplete in the following sense. For a quadratic discriminant Δ and a class $F \in \mathfrak{F}_\Delta$, we have seen that the basic characters $\sigma_j(F)$ only depend on the genus $F\mathfrak{F}_\Delta^2$, but we have not yet proved that in fact the genus of a class F is uniquely determined by the genus characters. To prove this, we must show that the group $\widehat{\mathfrak{F}_\Delta/\mathfrak{F}_\Delta^2}$ of all genus characters is generated by the basic genus characters. In classical terminology, this is the content of the subsequent duplication theorem of Gauss.

Theorem 6.5.11 (Gauss' duplication theorem)**.** *Let Δ be a quadratic discriminant and keep the terminology introduced in* Theorem 6.5.3. *Then*

$$\operatorname{Ker}(\boldsymbol{\sigma}_\Delta) = \operatorname{Ker}(\Psi_\Delta) = \mathfrak{F}_\Delta^2\,, \quad \textit{and} \quad \Psi_\Delta \quad \textit{is surjective.}$$

In particular, the following assertions hold:

1. $\widehat{\mathfrak{F}_\Delta/\mathfrak{F}_\Delta^2} = \langle \sigma_1, \ldots, \sigma_{\mu(\Delta)} \rangle$.
2. *If $m \in \mathbb{Z}$ and $\mathsf{Q}_\Delta(m) = 1$, then there exists a class $F \in \mathfrak{F}_\Delta$ which represents an integer $m_0 \in m + \Delta^*\mathbb{Z}$.*
3. *If $F \in \mathfrak{F}_\Delta$, then $\sigma_j(F) = 1$ for all $j \in [1, \mu(\Delta)]$ if and only if $F = G^2$ for some $G \in \mathfrak{F}_\Delta$. In particular, two classes F, $G \in \mathfrak{F}_\Delta$ lie in the same genus if and only if $\boldsymbol{\sigma}_\Delta(F) = \boldsymbol{\sigma}_\Delta(G)$.*
4. *If $F \in \mathfrak{F}_\Delta$ represents an integer m such that $(\Delta, m) = 1$, then $\mathsf{Q}_\Delta(m) = 1$, $\boldsymbol{\sigma}_\Delta(F) = \boldsymbol{\varphi}_\Delta(m + \Delta^*\mathbb{Z})$, and $F\mathfrak{F}_\Delta^2 \in \mathfrak{F}_\Delta/\mathfrak{F}_\Delta^2$ is the only genus which represents m. In particular, the genus which represents m is uniquely determined by the residue class $m + \Delta^*\mathbb{Z}$.*

PROOF. The main task is the proof of one of the following three assertions:

a. Ψ_Δ is surjective.
b. $\operatorname{Ker}(\boldsymbol{\sigma}_\Delta) \subset \mathfrak{F}_\Delta^2$.
c. $\operatorname{Ker}(\Psi_\Delta) \subset \mathfrak{F}_\Delta^2$.

Assume that one of these three assertions holds. Since $\boldsymbol{\sigma}_\Delta = \boldsymbol{\varphi}_\Delta^* \circ \Psi_\Delta$ and $\boldsymbol{\varphi}_\Delta^*$ is an isomorphism, it follows that $\mathrm{Ker}(\boldsymbol{\sigma}_\Delta) = \mathrm{Ker}(\Psi_\Delta)$, and since $\mathfrak{F}_\Delta^2 \subset \mathrm{Ker}(\Psi_\Delta)$, we obtain $\mathrm{Ker}(\boldsymbol{\sigma}_\Delta) = \mathrm{Ker}(\Psi_\Delta) = \mathfrak{F}_\Delta^2$, provided that **b.** or **c.** holds. By Theorem 6.5.3.4 we have $(\mathrm{Ker}(\mathsf{Q}_\Delta)/\mathcal{H}_\Delta : \Psi_\Delta(\mathfrak{F}_\Delta)) = (\mathrm{Ker}(\Psi_\Delta : \mathfrak{F}_\Delta^2)$, and therefore Ψ_Δ is surjective if and only if $\mathrm{Ker}(\Psi_\Delta) = \mathfrak{F}_\Delta^2$. Hence the conditions **a.**, **b.** and **c.** are equivalent.

Now it is easy to prove the assertions 1. to 4. using **a.**, **b.** and **c.**

1. Assume to the contrary that there is some $\phi \in \widehat{\mathfrak{F}_\Delta/\mathfrak{F}_\Delta^2} \setminus \langle \sigma_1, \ldots, \sigma_{\mu(\Delta)} \rangle$. By Theorem A.7.8.4, there exists a genus $F\mathfrak{F}_\Delta^2 \in \mathfrak{F}_\Delta/\mathfrak{F}_\Delta^2$ such that $\phi(F\mathfrak{F}_\Delta^2) \neq 1$, but $\sigma_j(F\mathfrak{F}_\Delta^2) = \sigma_j(F) = 1$ for all $j \in [1, \mu(\Delta)]$ and therefore $F \in \mathfrak{F}_\Delta^2$, a contradiction.

2. If $m \in \mathbb{Z}$ and $\mathsf{Q}_\Delta(m) = 1$, then $(\Delta, m) = 1$ and $m + \Delta^*\mathbb{Z} \in \mathrm{Ker}(\mathsf{Q}_\Delta)$. Since $\Psi_\Delta \colon \mathfrak{F}_\Delta \to \mathrm{Ker}(\mathsf{Q}_\Delta)/\mathcal{H}_\Delta$ is surjective, we obtain $m + \Delta^*\mathbb{Z} \in \psi_\Delta(F) = \mathcal{H}_F$ for some $F \in \mathfrak{F}_\Delta$, and therefore F represents an integer $m_0 \in m + \Delta^*\mathbb{Z}$.

3. Obvious, since $\mathrm{Ker}(\boldsymbol{\sigma}_\Delta) \subset \mathfrak{F}_\Delta^2$ implies $\mathrm{Ker}(\boldsymbol{\sigma}_\Delta) = \mathfrak{F}_\Delta^2$.

4. If F represents $m \in \mathbb{Z}$ and $(\Delta, m) = 1$, then $m + \Delta^*\mathbb{Z} \in \mathcal{H}_F \subset \mathrm{Ker}(\mathsf{Q}_\Delta)$, hence $\mathsf{Q}_\Delta(m) = 1$, and it follows by the very definition of $\boldsymbol{\sigma}_\Delta$ that $\boldsymbol{\sigma}_\Delta(F) = \boldsymbol{\varphi}_\Delta(m + \Delta^*\mathbb{Z})$. If $G \in \mathfrak{F}_\Delta$ is any class which represents m, then $\boldsymbol{\sigma}_\Delta(F) = \boldsymbol{\sigma}_\Delta(G)$, and therefore $F\mathfrak{F}_\Delta^2 = G\mathfrak{F}_\Delta^2$ by 3.

In the sequel we present Dirichlet's proof of **a.** and Mertens' proof of **c.** Later, in Section 6.6, we shall present Gauss' own proof of **c.**

1. (Dirichlet's proof) We prove **a.** Let $m \in \mathbb{Z}$ be such that $(\Delta, m) = 1$ and $m + \Delta^*\mathbb{Z} \in \mathrm{Ker}(\mathsf{Q}_\Delta)$. By Dirichlet's prime number theorem, there exists some prime p such that $p \equiv m \bmod \Delta^*\mathbb{Z}$. It follows that $\mathsf{Q}_\Delta(p) = \mathsf{Q}_\Delta(m) = 1$, hence Δ is a quadratic residue modulo $4p$, and therefore p is represented by some class $F \in \mathfrak{F}_\Delta$. Hence we obtain $\mathcal{H}_F = (p + \Delta^*\mathbb{Z})\mathcal{H}_\Delta = (m + \Delta^*\mathbb{Z})\mathcal{H}_\Delta = \Psi_\Delta(F)$. □

2. (Mertens' proof [**72**]) We prove **c.** We need some additional terminology. For a discriminant Δ, we denote by $r(\Delta)$ the number of odd primes dividing Δ, we define

$$D = \frac{\Delta}{4} \ \text{ if } \ \Delta \equiv 0 \bmod 4\,, \qquad D = \Delta \ \text{ if } \ \Delta \equiv 1 \bmod 4\,,$$

$$\tau(\Delta) = \begin{cases} r(\Delta) & \text{if } D \equiv 1 \bmod 2\,, \\ r(\Delta) + 1 & \text{if } D \equiv 0 \bmod 2\,, \end{cases} \qquad \text{and} \quad \mathsf{s}(\Delta) = \mu(\Delta) + \tau(\Delta)\,.$$

Then it follows that

$$\mu(\Delta) = \begin{cases} \tau(\Delta) + 1 & \text{if } \ D \equiv 3 \bmod 4 \ \text{ or } \ D \equiv 0 \bmod 8\,, \\ \tau(\Delta) & \text{otherwise,} \end{cases}$$

and

$$\mathsf{s}(\Delta) = \begin{cases} 2\tau(\Delta) + 1 = 2\mu(\Delta) - 1 & \text{if } \ D \equiv 3 \bmod 4 \ \text{ or } \ D \equiv 0 \bmod 8\,, \\ 2\tau(\Delta) = 2\mu(\Delta) & \text{otherwise,} \end{cases}$$

and we prove the assertion by induction on $\mathsf{s}(\Delta)$.

Suppose that $F \in \mathrm{Ker}(\boldsymbol{\sigma}_\Delta)$, hence $\sigma_j(F) = 1$ for all $j \in [1, \mu(\Delta)]$. We must prove that $F \in \mathfrak{F}_\Delta^2$, and (by the induction hypothesis) we suppose that the assertion holds for all quadratic discriminants Δ' such that $\mathsf{s}(\Delta') < \mathsf{s}(\Delta)$.

Case **I.** $\Delta \not\equiv 4 \bmod 16$. We prove first:

A. There exist integers $m \in \mathbb{N}$ and $b,\, c \in \mathbb{Z}$ such that $(m,b,c) = (2\Delta, m) = 1$ and $m = q_1 \cdot \ldots \cdot q_s$, where $s \in [0, \mu(\Delta) - 1]$, $q_1, \ldots, q_s$ are distinct primes, and $F \in [\![m,b,c]\!]\,\mathfrak{F}_\Delta^2$.

Proof of **A.** Suppose that $F \in \mathfrak{F}_\Delta$. Then F properly represents some $m_1 \in \mathbb{N}$ such that $(2\Delta, m_1) = 1$, and thus $F = [\![m_1, *, *]\!]$. We set $m_1 = e^2 q_1 \cdot \ldots \cdot q_t$, where $e \in \mathbb{N}$, $t \in \mathbb{N}_0$, and $q_1, \ldots, q_t$ are distinct odd primes. By Corollary 6.4.9, there is a factorization $F = E^2 * F_1 * \ldots * F_t$, where $E = [\![e,*,*]\!] \in \mathfrak{F}_\Delta$ and $F_j = [\![q_j, *, *]\!] \in \mathfrak{F}_\Delta$ for all $j \in [1,t]$. Since $\dim_{\mathbb{F}_2}(\mathfrak{F}_\Delta/\mathfrak{F}_\Delta^2) = \mu(\Delta) - 1$, there exist some $s \in \mathbb{N}_0$ and $G \in \mathfrak{F}_\Delta$ such that $s \le \min\{t, \mu(\Delta) - 1\}$, and (after renumbering if necessary) $F_1 * \ldots * F_t = F_1 * \ldots * F_s * G^2$. If $m = q_1 \cdot \ldots \cdot q_s$, then there exist $b,\, c \in \mathbb{Z}$ such that $F_1 * \ldots * F_s = [\![m,b,c]\!]$, and consequently $F \in [\![m,b,c]\!]\,\mathfrak{F}_\Delta^2$. $\square$[**A.**]

By **A**, we may assume that $F = [\![m,b,c]\!]$, where $m \in \mathbb{N}$, $(2\Delta, m) = 1$ and $m = q_1 \cdot \ldots \cdot q_s$ such that $s \in [0, \mu(\Delta) - 1]$ and $q_1, \ldots, q_s$ are distinct odd primes. If $m = 1$, then $F = H_\Delta$ by Theorem 6.2.1.3, and we are done. Thus suppose that $m > 1$. Then $4m$ is a quadratic discriminant, and if $m \equiv 1 \bmod 4$, then m itself is a quadratic discriminant.

Since $\sigma_j(F) = 1$ for all $j \in [1, \mu(\Delta)]$, the following conditions hold:

- $\Big(\dfrac{m}{p}\Big) = 1$ for all odd primes p dividing Δ.
- $m \equiv 1 \bmod 4$ if $D \equiv 3 \bmod 4$ or $D \equiv 4 \bmod 8$.
- $m \equiv \pm 1 \bmod 8$ if $D \equiv 2 \bmod 8$.
- $m \equiv 1$ or $3 \bmod 8$ if $D \equiv -2 \bmod 8$.
- $m \equiv 1 \bmod 8$ if $D \equiv 0 \bmod 8$.

Since $\Delta = b^2 - 4mc \equiv b^2 \bmod 4m$, it follows that Δ is a quadratic residue modulo $4m$ and D is a quadratic residue modulo m.

CASE 1: $D \equiv 0 \bmod 2$ and $m \equiv 1 \bmod 8$. Then m is a quadratic residue modulo $4|D|$, and there exist $u,\, v \in \mathbb{Z}$ such that $v^2 = m + 4Du$. Now $m = v^2 - 4Du$ is the discriminant of the form $g = [D, v, u]$, and as $(\Delta, m) = 1$, it follows that $(D, v) = 1$, g is primitive, and $G = [\![D, v, u]\!] \in \mathfrak{F}_m$. Since D is a quadratic residue modulo m, we get

$$\Big(\frac{D}{q_j}\Big) = 1 \quad \text{for all} \quad j \in [1,s]\,, \quad \text{and therefore} \quad G \in \operatorname{Ker}(\boldsymbol{\sigma}_m)\,.$$

Since $\mathsf{s}(m) = 2\tau(m) = 2s \le 2\mu(\Delta) - 2 < \mathsf{s}(\Delta)$, the induction hypothesis implies that $G \in \mathfrak{F}_m^2$. Hence there exists some $E \in \mathfrak{F}_m$ such that $H_m = E^2 * G$, and we may assume that $E = [\![e,*,*]\!]$, where $e \in \mathbb{N}$ and $(e, 2mD) = 1$. Then $H_m = [\![e^2D, *, *]\!]$ by Theorem 6.4.5.1, hence H_m properly represents e^2D, and there exist $x,\, y \in \mathbb{Z}$ such that

$$e^2D = g_m(x,y) = x^2 + xy + \frac{1-m}{4}\,y^2 \quad \text{and} \quad (x,y) = 1\,.$$

We obtain $(D, y) = 1$, hence $(\Delta, y) = 1$, and $my^2 = (2x+y)^2 - 4e^2D$. Suppose that $d = (2x+y, 2e)$, and let $x_1,\, y_1 \in \mathbb{Z}$ be such that $2x + y = dx_1$ and $2e = dy_1$. Then $(x_1, y_1) = 1$, $d^2 \,|\, my^2$, and $d \,|\, y$ since m is squarefree. Since $m(d^{-1}y)^2 = x_1^2 - Dy_1^2$

is properly represented by H_Δ, it follows that $H_\Delta = [\![m(d^{-1}y)^2, *, *]\!]$. By Theorem 6.4.5.1(a), there exists some $t \in \mathbb{N}$ such that $t \,|\, m$, and

$$F = F * H_\Delta = [\![m, b, c]\!] * [\![m(d^{-1}y)^2, *, *]\!] = [\![(t^{-1}md^{-1}y)^2, *, *]\!]\,.$$

Since $(\Delta, my) = 1$, we obtain $F \in \mathfrak{F}_\Delta^2$ by Theorem 6.4.11.

CASE 2: $D \equiv 1 \mod 2$ or $m \not\equiv 1 \mod 8$. Then m is a quadratic residue modulo $|D|$. Hence there exist u, $v \in \mathbb{Z}$ such that $v^2 = m + Du$, and as $(D, m) = 1$, it follows that $(D, v) = 1$. Now $4m = (2v)^2 - 4Du$ is the discriminant of the form $g = [D, 2v, u]$, and we assert that g is primitive. Assume the contrary. Then $(D, v) = 1$ implies $D \equiv u \equiv 0 \mod 2$, and therefore $m \not\equiv 1 \mod 8$. Since $m = v^2 - Du \equiv 1 \mod 4$, we obtain $m \equiv 5 \mod 8$ and $D \equiv 2 \mod 4$, a contradiction.

We set $G = [\![g]\!] = [\![D, 2v, u]\!] \in \mathfrak{F}_{4m}$, and we assert that $G \in \operatorname{Ker}(\boldsymbol{\sigma}_{4m})$. Since D is a quadratic residue modulo m, it follows that

$$\sigma_j(G) = \Big(\frac{D}{q_j}\Big) = 1 \quad \text{for all} \quad j \in [1, s]\,,$$

and if $m \equiv 1 \mod 4$, this implies $G \in \operatorname{Ker}(\boldsymbol{\sigma}_{4m})$.

Thus assume that $m \equiv 3 \mod 4$. By Theorem 6.5.5, we must prove that G represents some integer $n \equiv 1 \mod 4$, and since G represents D and u, it suffices to prove that either $D \equiv 1 \mod 4$ or $u \equiv 1 \mod 4$, and we assume that $D \not\equiv 1 \mod 4$. Then $D \equiv \pm 2 \mod 8$, and since $m = v^2 - Du$, it follows that $v \equiv u \equiv 1 \mod 2$. If $u \equiv 3 \mod 4$, then

$$m \equiv 1 - Du \equiv \begin{cases} 3 \mod 8 & \text{if} \quad D \equiv 2 \mod 8\,, \\ -1 \mod 8 & \text{if} \quad D \equiv -2 \mod 8\,, \end{cases}$$

a contradiction. Hence we obtain $u \equiv 1 \mod 4$ as asserted.

We want to apply the induction hypothesis for G. To do so, we make sure that $\mathsf{s}(4m) < \mathsf{s}(\Delta)$. If $m \equiv 1 \mod 4$, then $\mathsf{s}(4m) = 2\tau(m) = 2s \le 2\mu(\Delta) - 2 < \mathsf{s}(\Delta)$. If $m \equiv 3 \mod 4$, then (observing that $D \not\equiv 3 \mod 4$ and $D \not\equiv 0 \mod 8$), we obtain $\mathsf{s}(4m) = 2\tau(m) + 1 \le 2\mu(\Delta) - 1 < \mathsf{s}(\Delta) = 2\mu(\Delta)$.

The induction hypothesis implies that $G \in \mathfrak{F}_{4m}^2$, and therefore there exists some $E \in \mathfrak{F}_{4m}$ such that $H_{4m} = E^2 * G$, and (as above) we may assume that $E = [\![e, *, *]\!]$, where $e \in \mathbb{N}$, $(e, 2mD) = 1$, and $H_{4m} = [\![e^2D, *, *]\!]$. Hence g_{4m} properly represents e^2D, and therefore there exist x, $y \in \mathbb{Z}$ such that $e^2D = g_{4m}(x, y) = x^2 - my^2$ and $(x, y) = 1$. It follows that $(D, y) = 1$, and we assert that $(\Delta, y) = 1$. This is obvious if $\Delta = D$ or if $D \equiv 0 \mod 2$. However, if $\Delta = 4D$ and $D \equiv 1 \mod 2$, then we have $D \equiv 3 \mod 4$ (as we are in Case **I**), and we obtain $3 \equiv e^2D \equiv x^2 - my^2 \mod 4$, which implies $y \equiv 1 \mod 2$ and thus $(\Delta, y) = 1$.

If $\Delta = 4D$, then $g_\Delta(x, e) = x^2 - e^2D = my^2$, and if $\Delta = D \equiv 1 \mod 4$, then

$$g_\Delta(x - e, 2e) = (x - e)^2 + 2e(x - e) + \frac{1 - D}{4}\,(2e)^2 = x^2 - e^2D = my^2\,.$$

In any case, there exist x_1, $y_1 \in \mathbb{Z}$ such that $g_\Delta(x_1, y_1) = my^2$, and if $d = (x_1, y_1)$, then $d^2 \,|\, my^2$ and therefore $d \,|\, y$, since m is squarefree. We obtain

$$\Big(\frac{x_1}{d}, \frac{y_1}{d}\Big) = 1 \quad \text{and} \quad g_\Delta\Big(\frac{x_1}{d}, \frac{y_1}{d}\Big) = m(d^{-1}y)^2\,.$$

Hence it follows that $H_\Delta = \llbracket m(d^{-1}y)^2,*,*\rrbracket$, and (as above) there exists some $t \in \mathbb{N}$ such that $t \,|\, m(d^{-1}y)^2$, and

$$F = F * H_\Delta = \llbracket m,b,c\rrbracket * \llbracket m(d^{-1}y)^2,*,*\rrbracket = \llbracket (t^{-1}md^{-1}y)^2,*,*\rrbracket \in \mathfrak{F}_\Delta^2\,.$$

Case **II.** $\Delta \equiv 4 \bmod 16$. In this case, $\Delta = 4D$, where $D \equiv 1 \bmod 4$, and we apply Theorem 6.4.14. We consider the epimorphism $\Theta = \Theta_{D,2}\colon \mathfrak{F}_\Delta \to \mathfrak{F}_D$, and we assume that $F \in \operatorname{Ker}(\boldsymbol{\sigma}_\Delta) \subset \mathfrak{F}_\Delta$. Then $F = \llbracket a,2b,4c\rrbracket$ for some a, b, $c \in \mathbb{Z}$ such that $(\Delta,a)=1$, $(a,b,c)=1$, and $\Theta(F) = \llbracket a,b,c\rrbracket$. Since

$$\boldsymbol{\sigma}_\Delta(F) = \Big(\Big(\frac{a}{q_1}\Big),\ldots,\Big(\frac{a}{q_r}\Big)\Big) = \boldsymbol{\sigma}_D(\Theta(F))\,,$$

it follows that $\Theta(F) \in \operatorname{Ker}(\boldsymbol{\sigma}_D)$ and, by Case **I**, we get $\Theta(F) = F_0^2$ for some $F_0 \in \mathfrak{F}_D$. Let $F_1 \in \mathfrak{F}_\Delta$ be such that $\Theta(F_1) = F_0$. Then $\Theta(F_1^2 * F^{-1}) = H_D$, and since $|\operatorname{Ker}(\Theta)| \in \{1,3\}$, it follows that $(F_1^2 * F^{-1})^3 = H_\Delta$, and $F = (F_1 * F^{-1})^2 \in \mathfrak{F}_\Delta^2$. $\square$

By Theorem 6.5.11, the homomorphism $\boldsymbol{\sigma}_\Delta\colon \mathfrak{F}_\Delta \to \{\pm1\}^{\mu(\Delta)}$ is not surjective (indeed, $\operatorname{Ker}(\boldsymbol{\sigma}_\Delta = \mathfrak{F}^2$, and $|\mathfrak{F}_\Delta/\mathfrak{F}_\Delta^2| = 2^{\mu(\Delta)-1}$). In the following Theorems 6.5.12 and 6.5.13 we investigate the image of $\boldsymbol{\sigma}_\Delta$ in two important special cases (compare with the phenomena which arose in the Examples 6.5.6, 6.5.7 and 6.5.8).

Theorem 6.5.12. *Let Δ be a quadratic discriminant of the form $\Delta = 2^eD$, where $e \in \{0,2,3\}$ and $D \in \mathbb{Z}$ is odd and squarefree.*

1. *If $F \in \mathfrak{F}_\Delta$, then*
$$\prod_{j=1}^{\mu(\Delta)} \sigma_j(F) = 1\,.$$
2. *Let F, $G \in \mathfrak{F}_\Delta$ and m, $n \in \mathbb{Z}$ be such that $(\Delta,m) = (\Delta,n) = 1$, F represents m and G represents n. Then F and G lie in the same genus if and only if*
$$\Big(\frac{m}{p}\Big) = \Big(\frac{n}{p}\Big) \quad \textit{for all odd primes } p \textit{ dividing } D\,.$$

Proof. Suppose that $|D| = p_1 \cdot \ldots \cdot p_r$, where $r \in \mathbb{N}_0$, $p_1,\ldots,p_r$ are distinct odd primes, and consider a class $F \in \mathfrak{F}_\Delta$. Since F properly represents some integer $m \in \mathbb{N}$ such that $(\Delta,m) = 1$, we may assume that

$$F = \llbracket m,*,*\rrbracket\,, \quad \text{where} \quad m \in \mathbb{N}\,,\ (\Delta,m) = 1 \quad \text{and} \quad \Big(\frac{\Delta}{m}\Big) = 1\,.$$

Let $\sigma_1,\ldots,\sigma_r,\,\varepsilon,\,\delta\colon \mathfrak{F}_\Delta \to \{\pm1\}$ be given by

$$\sigma_i(F) = \Big(\frac{m}{p_i}\Big) \ \text{ for } i \in [1,r]\,,\ \varepsilon(F) = \Big(\frac{-1}{m}\Big) \ \text{ if } e \ne 0\,,\ \text{ and } \delta(F) = \Big(\frac{2}{m}\Big) \ \text{ if } e = 3\,.$$

1. CASE 1: $e \in \{0,2\}$, $D \equiv 1 \bmod 4$, $\mu(\Delta) = r$, $\boldsymbol{\sigma}_\Delta = (\sigma_1,\ldots,\sigma_r)$. Then
$$\prod_{j=1}^{\mu(\Delta)} \sigma_j(F) = \prod_{j=1}^{r}\Big(\frac{m}{p_j}\Big) = \Big(\frac{m}{|D|}\Big) = \Big(\frac{D}{m}\Big) = \Big(\frac{\Delta}{m}\Big) = 1\,.$$

CASE 2: $e=2$, $D\equiv 3 \bmod 4$, $\mu(\Delta)=r+1$, $\boldsymbol{\sigma}_\Delta=(\sigma_1,\ldots,\sigma_r,\varepsilon)$. Then

$$\prod_{j=1}^{\mu(\Delta)}\sigma_j(F)=\prod_{j=1}^{r}\Bigl(\frac{m}{p_j}\Bigr)(-1)^{(m-1)/2}=\Bigl(\frac{m}{|D|}\Bigr)(-1)^{(m-1)/2}=\Bigl(\frac{D}{m}\Bigr)=\Bigl(\frac{\Delta}{m}\Bigr)=1\,.$$

CASE 3: $e=3$, $D\equiv 1 \bmod 4$, $\mu(\Delta)=r+1$, $\boldsymbol{\sigma}_\Delta=(\sigma_1,\ldots,\sigma_r,\delta)$. Then

$$\prod_{j=1}^{\mu(\Delta)}\sigma_j(F)=\prod_{j=1}^{r}\Bigl(\frac{m}{p_j}\Bigr)\Bigl(\frac{2}{m}\Bigr)=\Bigl(\frac{m}{|D|}\Bigr)\Bigl(\frac{2}{m}\Bigr)=\Bigl(\frac{D}{m}\Bigr)\Bigl(\frac{2}{m}\Bigr)=\Bigl(\frac{\Delta}{m}\Bigr)=1\,.$$

CASE 4: $e=3$, $D\equiv 3 \bmod 4$, $\mu(\Delta)=r+1$, $\boldsymbol{\sigma}_\Delta=(\sigma_1,\ldots,\sigma_r,\varepsilon\delta)$. Then

$$\prod_{j=1}^{\mu(\Delta)}\sigma_j(F)=\prod_{j=1}^{r}\Bigl(\frac{m}{p_j}\Bigr)\Bigl(\frac{-2}{m}\Bigr)=\Bigl(\frac{m}{|D|}\Bigr)\Bigl(\frac{-2}{m}\Bigr)=\Bigl(\frac{D}{m}\Bigr)\Bigl(\frac{2}{m}\Bigr)=\Bigl(\frac{\Delta}{m}\Bigr)=1\,.$$

2. By Theorem 6.5.5,

$$\Bigl(\frac{m}{p}\Bigr)=\Bigl(\frac{n}{p}\Bigr)\quad\text{for all odd primes } p \text{ dividing } \Delta$$

holds if and only if $\sigma_j(F)=\sigma_j(G)$ for all $j\in[1,r]$, and by 1. this is equivalent to $\boldsymbol{\sigma}_\Delta(F)=\boldsymbol{\sigma}_\Delta(G)$. Now the assertion follows by Theorem 6.5.11.3. □

Theorem 6.5.13. *Let $\Delta=2^eD$ be a quadratic discriminant, where $D\in\mathbb{Z}$ and $|D|=p_1^{e_1}\cdot\ldots\cdot p_r^{e_r}$ for some $r\in\mathbb{N}$, $e_1,\ldots,e_r\in\mathbb{N}$ and distinct odd primes $p_1,\ldots,p_r$. Then the following assertions are equivalent:*

(a) *For every $(\delta_1,\ldots,\delta_r)\in\{\pm1\}^r$, there exists some class $F\in\mathfrak{F}_\Delta$ such that $\sigma_j(F)=\delta_j$ for all $j\in[1,r]$.*

(b) *$e\ge 2$, and if $e\equiv 0 \bmod 2$, then $D\equiv 3 \bmod 4$.*

PROOF. Recall that $\boldsymbol{\sigma}_\Delta=\boldsymbol{\varphi}_\Delta^*\circ\Psi_\Delta\colon\mathfrak{F}_\Delta\to\{\pm1\}^{\mu(\Delta)}$, $\Psi_\Delta\colon\mathfrak{F}_\Delta\overset{\sim}{\to}\mathrm{Ker}(\mathsf{Q}_\Delta)/\mathcal{H}_\Delta$ is an isomorphism, and $\boldsymbol{\varphi}_\Delta^*$ is induced by

$$\boldsymbol{\varphi}_\Delta=(\chi_1,\ldots,\chi_{\mu(\Delta)})\colon(\mathbb{Z}/\Delta^*\mathbb{Z})^\times\to\{\pm1\}^{\mu(\Delta)}\,,$$

where

$$\chi_j(m+\Delta^*\mathbb{Z})=\Bigl(\frac{m}{p_j}\Bigr)\quad\text{for } m\in\mathbb{N} \text{ such that } (\Delta,m)=1.$$

Hence (a) is equivalent $(\sigma_1,\ldots,\sigma_r)(\mathrm{Ker}(\mathsf{Q}_\Delta))=\{\pm1\}^r$. If $m+\Delta^*\mathbb{Z}\in\mathrm{Ker}(\mathsf{Q}_\Delta)$, where $m\in\mathbb{N}$ and $(\Delta,m)=1$, then

$$\mathsf{Q}_\Delta(m)=\Bigl(\frac{\Delta}{m}\Bigr)=\Bigl(\frac{2^eD}{m}\Bigr)=\Bigl(\frac{2}{m}\Bigr)^e\Bigl(\frac{m}{|D|}\Bigr)=\Bigl(\frac{2}{m}\Bigr)^e(-1)^{\frac{m-1}{2}\,\frac{D-1}{2}}\prod_{j=1}^{r}\Bigl(\frac{m}{p_j}\Bigr)^{e_j}.$$

Hence (a) holds if and only if, for every $(\delta_1,\ldots,\delta_r)\in\{\pm1\}^r$, there exists some $m\in\mathbb{N}$ such that $(\Delta,m)=1$ and

$$\phi_D(m)=\Bigl(\frac{2}{m}\Bigr)^e(-1)^{\frac{m-1}{2}\,\frac{D-1}{2}}=\prod_{j=1}^{r}\delta_j^{e_j}\,.$$

CASE 1: $e_j \equiv 0 \bmod 2$ for all $j \in [1, r]$. Then $|D|$ is a square, thus $e \geq 2$, and

- $D \equiv 1 \bmod 4$ and $e \equiv 1 \bmod 2$ if $D > 0$;
- $D \equiv 3 \bmod 4$ if $D < 0$.

Hence (b) holds, and we must prove that there is some positive integer m such that $(\Delta, m) = 1$ and $\phi_D(m) = 1$. It is sufficient to set

$$m \equiv \begin{cases} 1 \mod 8 & \text{if} \quad D > 0\,, \\ 3 \mod 8 & \text{if} \quad D < 0,\ e \equiv 1 \mod 2\,, \\ 1 \mod 4 & \text{if} \quad D < 0,\ e \equiv 0 \mod 2\,. \end{cases}$$

CASE 2: $e_j \equiv 1 \bmod 2$ for some $j \in [1, r]$. In this case, (a) holds if and only if there exist positive integers m_+, m_- such that $(\Delta, m_\pm) = 1$ and $\phi_D(m_\pm) = \pm 1$.

Assume that (b) fails. Since $e = 0$ implies $D \equiv 1 \bmod 4$, we obtain in any case $e \equiv 0 \bmod 2$ and $D \equiv 1 \bmod 4$. But then it follows that $\phi_D(m) = 1$ for all $m \in \mathbb{N}$ such that $(\Delta, m) = 1$. Hence (a) fails, too.

Thus suppose that (b) holds. Then we obtain

$$\phi_D(m) = \begin{cases} \left(\frac{-1}{m}\right) & \text{if} \quad e \equiv 0 \mod 2 \quad \text{and} \quad D \equiv 3 \mod 4\,, \\ \left(\frac{2}{m}\right) & \text{if} \quad e \equiv 1 \mod 2 \quad \text{and} \quad D \equiv 1 \mod 4\,, \\ \left(\frac{-2}{m}\right) & \text{if} \quad e \equiv 0 \mod 2 \quad \text{and} \quad D \equiv 3 \mod 4\,, \end{cases}$$

and in each case there exist positive integers $m_\pm$ such that $\phi_D(m_\pm) = \pm 1$. □

Exercise 6.5.14. Let Δ be a quadratic discriminant and ϕ a genus character of discriminant Δ. Prove that there exists a quadratic discriminant Δ_ϕ with the following properties: $\Delta_\phi \,|\, \Delta$, and if $F \in \mathfrak{F}_\Delta$ represents some integer m such that $(\Delta, m) = 1$, then $\phi(F) = \mathsf{Q}_{\Delta_\phi}(m)$.

The examples 6.5.6 and 6.5.7 as well as the discriminants of Exercise 6.5.9 show the simplicity of discriminants having only one class in each genus. Negative even discriminants with this property have several other interesting features and were already used by L. Euler to identify large primes. We give the following definition in the spirit of Euler's application.

> A positive integer n is called a *convenient number* (numerus idoneus) if it has the following property: Whenever an odd integer $m > 1$ has only one representation in the form $m = a^2 + nb^2$, where $a,\ b \in \mathbb{N}$ and $(a, b) = 1$, then m is a prime power.

(For $n = 1$, in this definition the representations $m = a^2 + b^2$ and $m = b^2 + a^2$ are considered to be equal.)

Euler himself used (among others) the convenient number 1848 to prove that

$$18,518.809 = 197^2 + 1848 \cdot 100^2$$

is a prime! There is a wealth of interesting results on convenient numbers. Gauss listed 65 convenient numbers, and it is conjectured that these are all (see the tables in [**19**, p. 60] and [**27**, Table B2]). We refer the interested reader to the survey article [**28**] and to http://oeis.org/A000926. Here we restrict to the connection with class groups. The proof of the following Theorem 6.5.15 is is a modification of that given in [**61**].

Theorem 6.5.15. *A positive integer* n *is convenient if and only if* $\mathfrak{F}_{-4n}$ *is an elementary* 2*-group.*

Proof. Let n be a positive integer, $\Delta = -4n$, $H = [\![1,0,n]\!]$ the principal class of discriminant Δ, $|\mathfrak{F}_\Delta| = h$, and suppose that $\mathfrak{F}_\Delta = \{\,[\![f_1]\!],\ldots,\,[\![f_h]\!]\}$. If a positive integer m such that $(\Delta, m) = 1$ is properly represented by some class of $\mathfrak{F}_\Delta$, then Theorem 6.2.12.2 implies that

$$\Psi_\Delta(m) = \sum_{i=1}^{h} \big|\{(x,y)\in\mathbb{Z}^2 \mid (x,y)=1,\ f_i(x,y)=m\}\big| = \begin{cases} 2^{r+1} & \text{if} \quad n \ne 1\,, \\ 2^{r+2} & \text{if} \quad n = 1\,, \end{cases}$$

where r is the number of distinct primes dividing m.

Assume first that $\mathfrak{F}_\Delta$ is an elementary 2-group, and let $m > 1$ be an odd integer which has only one representation in the form $m = a^2 + nb^2$, where $a,\, b \in \mathbb{N}$ and $(a,b) = 1$. Since every genus consists of a single class, Theorem 6.5.11.3 implies that the principal class is the only class which represents m. Hence we obtain $\Psi_\Delta(m) \le 4$ if $n \ne 1$, and $\Psi_\Delta(m) \le 8$ if $n = 1$. Therefore it follows that $m = p^k$ for some prime p and $k \in \mathbb{N}$.

Assume now that $\mathfrak{F}_\Delta$ is not an elementary 2-group. It suffices to prove the following assertion:

A. There is a class $F \in \mathfrak{F}_\Delta$ such that $F^2 \ne H$ and F represents infinitely many primes.

Suppose that **A** holds. Then F represents two distinct odd primes p and q such that $(\Delta,p) = (\Delta,q) = 1$, F^{-1} also represents q, and by Corollary 6.4.8.2 it follows that the classes F^2 that $H = F * F^{-1}$ both properly represent pq. Suppose that $f_1 = [1,0,n]$ (hence $[\![f_1]\!] = H$) and $f_2 \in F^2$. Then it follows that

$$|\{(x,y)\in\mathbb{Z}^2 \mid (x,y)=1,\ f_i(x,y)=pq\}| \ge 4 \quad \text{for } i \in \{1,2\},$$

and since $\Psi_\Delta(pq) = 8$, we obtain $|\{(x,y)\in\mathbb{Z}^2 \mid (x,y)=1,\ x^2+ny^2=pq\}| = 4$. Hence pq has a unique representation $pq = a^2 + nb^2$, where $a,\, b \in \mathbb{N}_0$, and therefore n is not convenient.

Proof of **A.** Let $F_1 \in \mathfrak{F}_\Delta$ be a class such that $F_1^2 \ne H$. By Theorem 6.2.1.3, there exists a sequence $(m_i)_{i\ge1}$ of pairwise coprime positive integers such that $(\Delta, m_i) = 1$ and F_1 properly represents m_i for all $i \ge 1$. We set $m_i = p_{i,1}\cdot\ldots\cdot p_{i,k_i}$, where $k_i \ge$ and $p_{i,1},\ldots,p_{i,k_i}$ are (not necessarily distinct) primes. By Corollary 6.4.9, there exists for every $i \ge 1$ a factorization $F_1 = F_{i,1} * \ldots * F_{i,k_i}$ such that $F_{i,l} = [\![p_{i,l},*,*]\!] \in \mathfrak{F}_\Delta$ for all $l \in [1,k_i]$, and as $F_1^2 \ne H$, there exists some $l \in [1,k_i]$ such that $F_{i,l}^2 \ne H$. In particular, there exist infinitely many primes $p \in \{p_{i,l} \mid i \ge 1,\ l \in [1,k_i]\}$ represented by some class $F \in \mathfrak{F}_\Delta$ such that $F^2 \ne H$. Since $\mathfrak{F}_\Delta$ is finite and $p_{i,l} \ne p_{j,m}$ whenever $i \ne j$, the assertion follows. □

Exercise 6.5.16. Let n be a positive integer. Prove the equivalence of the following assertions :

a) n is convenient.

b) Any two improperly equivalent forms of discriminant $-4n$ are equivalent.

c) n is not of the form $ab+bc+ca$ with integers $0<a<b<c$.

Hint for the proof of the equivalence of **b)** and **c)**. $(a,b,c)\mapsto(b,a-b,c-b)$ defines a bijective map from the set of improper equivalence classes of forms of discriminant $-4n$ of order greater than 2 onto the set of all triples (d,e,f) with $d<e<f$ (see http://oeis.org/A000926/a000926.txt).

We close this section with a classical result due to A.-M. Legendre. In fact, Legendre gave an elementary proof of this result and used it for a partial proof of the quadratic reciprocity law. We refer to [**67**, Ch. I] for a thorough discussion of the historical development and further references. Here we make full use of Gauss' theory of quadratic forms to give a short and concise proof of Legendre's theorem. Note however, that Dirichlet deduced the duplication theorem from Legendre's theorem (see [**23**, §158]).

Theorem 6.5.17 (Legendre's theorem)**.** *Let a, b, c be non-zero integers such that*

- $(a,b)=(b,c)=(c,a)=1$*;*
- *a, b and c do not all have the same sign;*
- *$-bc$ is a quadratic residue modulo $|a|$, $-ca$ is a quadratic residue modulo $|b|$, and $-ab$ is a quadratic residue modulo $|c|$;*

Then there exists some $(x,y,z)\in\mathbb{Z}^3\setminus\{(0,0,0)\}$ such that $ax^2+by^2+cz^2=0$.

Proof. We may assume that a, b and c are squarefree. Indeed, suppose that the assertion is proved in this case, and set $a=a_0a_1^2$, $b=b_0b_1^2$ and $c=c_0c_1^2$, where a_0, b_0, $c_0\in\mathbb{Z}$ are squarefree, and a_1, b_1, $c_1\in\mathbb{Z}$. Then the assumptions of the theorem are satisfied for (a_0,b_0,c_0). If $(x_0,y_0,z_0)\in\mathbb{Z}^3\setminus\{(0,0,0)\}$ is such that $a_0x_0^2+b_0y_0^2+c_0z_0^2=0$, then $(x_0b_1c_1,y_0a_1c_1,z_0a_1b_1)\in\mathbb{Z}^3\setminus\{(0,0,0)\}$, and $a(x_0b_1c_1)^2+b(y_0a_1c_1)^2+c(z_0a_1b_1)^2=(a_0x_0^2+b_0y_0^2+c_0z_0^2)(a_1b_1c_1)^2=0$.

Let now a, b and c be squarefree. We may interchange the three number a, b, c, and we may also replace (a,b,c) by $(-a,-b,-c)$. This allows us to make the following additional assumptions.

If $2\nmid abc$, then $(-ab)(-bc)(-ac)=-(abc)^2\equiv-1 \bmod 4$, and we may assume that $-ac\equiv-1 \bmod 4$ and $a<0$. If $2\,|\,abc$, then we may assume that $2\,|\,ac$ and $a<0$. In any case, we may assume that $-4ac$ is a fundamental discriminant and $(4ac,b)=1$.

Since $-4ac$ is a quadratic residue modulo $4|b|$, Theorem 6.2.4.1 implies that b is represented by some class $F\in\mathfrak{F}_{-4ac}$. We consider the class $F_0=[\![-a,0,-c]\!]\in\mathfrak{F}_{-4ac}$ and a positive integer m such that $(4ac,m)=1$ which is represented by F_0, say $m=-ax^2-cy^2$ for some x, $y\in\mathbb{Z}$. We assert that F and F_0 lie in the same genus. By Theorem 6.5.12.2 we must prove that

$$\Big(\frac{b}{p}\Big)=\Big(\frac{m}{p}\Big)\quad\text{for all odd primes } p \text{ dividing } ac\,.$$

Thus let p be an odd prime dividing ac. If $p \,|\, a$, then

$$\Big(\frac{-bc}{p}\Big) = 1\,, \quad \text{and} \quad \Big(\frac{b}{p}\Big) = \Big(\frac{-c}{p}\Big) = \Big(\frac{-ax^2 - cy^2}{p}\Big) = \Big(\frac{m}{p}\Big)\,.$$

If $p \,|\, c$, then

$$\Big(\frac{-ab}{p}\Big) = 1\,, \quad \text{and} \quad \Big(\frac{b}{p}\Big) = \Big(\frac{-a}{p}\Big) = \Big(\frac{-ax^2 - cy^2}{p}\Big) = \Big(\frac{m}{p}\Big)\,.$$

Let $G \in \mathfrak{F}_{-4ac}$ such that $F * G^2 = F_0$, and let z be a non-zero integer represented by G. By Corollary 6.4.8.1, bz^2 is represented by F_0, and thus there exist $x,\, y \in \mathbb{Z}$ such that $bz^2 = -ax^2 - cy^2$. $\square$

6.6. Ternary quadratic forms

In this section, we give a brief account of Gauss' theory of ternary quadratic form to the extent that we can present Gauss' proofs of the duplication theorem and the three squares theorem. We follow the presentation given in [**27**]. For a more elaborate discussion of the material we refer to [**104**].

We start with some definitions from the elementary theory of ternary forms.

The *cofactor matrix* $A^\#$ of a matrix $A \in \mathsf{M}_3(\mathbb{Q})$ is defined as follows.

$$\text{If} \quad A = \begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix}\,, \quad \text{then} \quad A^\# = \begin{pmatrix} b'c'' - b''c' & c'a'' - c''a' & a'b'' - a''b' \\ b''c - bc'' & c''a - ca'' & a''b - ab'' \\ bc' - b'c & ca' - c'a & ab' - a'b \end{pmatrix}.$$

It is easily checked that the cofactor matrix has the following properties:

1. $(A^{\mathsf{t}})^\# = (A^\#)^{\mathsf{t}}$. In particular, if A is symmetric, then so is $A^\#$.
2. If $B \in \mathsf{M}_3(\mathbb{Q})$, then $(AB)^\# = A^\# B^\#$.
3. $(A^\#)^\# = \det(A)\, A$.
4. If $\det(A) \neq 0$, then $A^\# = \det(A)\, (A^{-1})^{\mathsf{t}}$, and $\det(A^\#) = \det(A)^2$.

Definition 6.6.1.

1. A *ternary form* is a homogeneous quadratic polynomial $\phi \in \mathbb{Z}[X, Y, Z]$. We write ϕ in the form

$$\phi = \phi(X, Y, Z) = aX^2 + bY^2 + cZ^2 + 2uXY + 2vYZ + 2wXZ\,,$$

where $a,\, b,\, c \in \mathbb{Z}$ and $u,\, v,\, w \in \frac{1}{2}\mathbb{Z}$. We call ϕ *classical* if $u,\, v,\, w \in \mathbb{Z}$.

With a ternary form ϕ as above we associate the matrix

$$M_\phi = \begin{pmatrix} a & u & w \\ u & b & v \\ w & v & c \end{pmatrix} \quad \text{and its cofactor matrix} \quad M_\phi^\# = \begin{pmatrix} A & U & W \\ U & B & V \\ W & V & C \end{pmatrix}\,,$$

where

$$A = bc - v^2\,, \quad B = ac - w^2\,, \quad C = ab - u^2\,,$$
$$U = vw - uc\,, \; V = uw - av\,, \; W = uv - bw\,.$$

We call $\delta_\phi = \det M_\phi$ the *determinant* of ϕ. Using its matrix M_ϕ, we may ϕ write in the form

$$\phi = (X,\,Y,\,Z)\,M_\phi \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}.$$

ϕ is said to *represent* an integer $m \in \mathbb{Z}$ if there exist $x,\,y,\,z \in \mathbb{Z}$ such that $m = \phi(x,y,z)$.

2. For a ternary form $\phi \in \mathbb{Z}[X,Y,Z]$ and a matrix $T \in \mathsf{GL}_3(\mathbb{Z})$ we define its transform by

$$T\phi = \phi\big((X,Y,Z)T\big) = (X,\,Y,\,Z)\,T\,M_\phi\,T^{\mathsf{t}} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} \in \mathbb{Z}[X,Y,Z]\,.$$

Obviously, $T\phi$ is a ternary form, and $M_{T\phi} = T\,M_\phi\,T^{\mathsf{t}}$. Two ternary forms ϕ and ψ are called *equivalent* if there exists a matrix $T \in \mathsf{GL}_3(\mathbb{Z})$ such that $\psi = T\phi$. If $\varepsilon_1,\,\varepsilon_2,\,\varepsilon_3 \in \{\pm 1\}$ and (X_1,Y_1,Z_1) is any permutation of (X,Y,Z), then $\phi = \phi(X,Y,Z)$ is equivalent to $\phi(\varepsilon_1X_1,\varepsilon_2X_2,\varepsilon_3X_3)$.

Equivalence is an equivalence relation on the set of ternary forms. Two equivalent forms f and g have the same determinant, represent the same integers, and both f and g are either classical or not. Note that there is no need for a distinction between proper and improper equivalence since the matrices T and $-T$ perform the same transformation, and $\det(-T) = -\det(T)$.

As for binary forms, we look for distinguished representatives in each equivalence class of ternary forms. In the following Theorem 6.6.2 we summarize the results of Gauss' reduction process.

Theorem 6.6.2 (Gauss' reduction of ternary forms)**.** *Every ternary form with determinant $\delta \neq 0$ is equivalent to a form*

$$\phi = aX^2 + bY^2 + cZ^2 + 2uXY + 2vYZ + 2wXZ\,,$$

where $a,\,b,\,c \in \mathbb{Z}$ and $u,\,v,\,w \in \frac{1}{2}\mathbb{Z}$ have the following properties:

If $C = ab - u^2$, $V = uw - av$ and $e = (2b, 2w)$, then

$$|a| \le 2\sqrt{\frac{|C|}{3}}\,, \quad |C| \le 2\sqrt{\frac{|a\delta|}{3}}\,, \quad |a| \le \frac{4}{3}\sqrt[3]{|\delta|}\,,$$

and

- *either* $aC \neq 0\,,\ -|a| < 2u \le |a|,\ 2|w| \le |a|$ *and* $-|C| < 2|V| \le |C|$,
- *or* $a = C = u = 0,\ \delta = -bw^2,\ -|w| < c \le |w|$ *and* $-e < 4v \le e$.

The proof of Theorem 6.6.2 depends on the following elementary Lemma 6.6.3 from the theory of binary forms.

Lemma 6.6.3. *If $a,\, c \in \mathbb{Z}$ and $b \in \frac{1}{2}\mathbb{Z}$, then there exist matrices $S,\, S_1 \in \mathsf{SL}_2(\mathbb{Z})$ such that*

$$S\begin{pmatrix} a & b \\ b & c\end{pmatrix}S^{\mathsf{t}} = \begin{pmatrix} a' & b' \\ b' & c'\end{pmatrix} \quad \text{and} \quad S_1\begin{pmatrix} a & b \\ b & c\end{pmatrix}S_1^{\mathsf{t}} = \begin{pmatrix} a_1' & b_1' \\ b_1' & c_1'\end{pmatrix},$$

where

$$|a'| \le 2\sqrt{\frac{|ac-b^2|}{3}} \quad \text{and} \quad |c_1'| \le 2\sqrt{\frac{|ac-b^2|}{3}}\,.$$

Proof of Lemma 6.6.3. We consider the form $f=[a,2b,c]$ of discriminant $\Delta = 4b^2-4ac$. It suffices to prove the existence of a form $f'=[a',2b',c']$ such that $|a'| \le 2\sqrt{|ac-b^2|/3}$ and f' is equivalent to f. Indeed, if this is done, let $S \in \mathsf{SL}_2(\mathbb{Z})$ be such that $f' = Sf$, and set

$$S_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0\end{pmatrix} S\,.$$

Then it follows that

$$S\begin{pmatrix} a & b \\ b & c\end{pmatrix}S^{\mathsf{t}} = \begin{pmatrix} a' & b' \\ b' & c'\end{pmatrix} \quad \text{and} \quad S_1\begin{pmatrix} a & b \\ b & c\end{pmatrix}S_1^{\mathsf{t}} = \begin{pmatrix} c' & -b' \\ -b' & a'\end{pmatrix}.$$

If f is degenerate, then f is equivalent to a form $f'=[0,2b',c']$ by Theorem 6.1.3.

If f is positive definite, then f is equivalent to a reduced form $f'=[a',2b',c']$, and by Theorem 6.3.2.1 we obtain $|a'| < \sqrt{|\Delta|/3} = 2\sqrt{|ac-b^2|/3}$. If f is negative definite, then $-f$ is positive definite, and if $-f$ is equivalent to $[a',2b',c']$, then f is equivalent to $[-a',-2b',-c']$.

If f is indefinite, then Theorem 6.3.6.2 implies that f is equivalent to a reduced form $f'=[a',2b',c']$ such that $|a'| < \sqrt{\Delta}/2 < \sqrt{\Delta/3} = 2\sqrt{|ac-b^2|/3}$. ☐

Proof of Theorem 6.6.2. Let ψ be a ternary form with determinant $\delta \ne 0$. We choose a ternary form ϕ_1 which is equivalent to ψ and whose matrix and cofactor matrix are given by

$$M_{\phi_1} = \begin{pmatrix} a & u_1 & w_1 \\ u_1 & b_1 & v_1 \\ w_1 & v_1 & c_1\end{pmatrix} \quad \text{and} \quad (M_{\phi_1})^{\#} = \begin{pmatrix} A_1 & U_1 & W_1 \\ U_1 & B_1 & V_1 \\ W_1 & V_1 & C\end{pmatrix}$$

such that $|a|+|C|$ is minimal among all ternary forms which are equivalent to ψ. As $(M_{\phi_1}^{\#})^{\#} = \delta M_{\phi_1}$, we obtain $a\delta = B_1C - V_1^2$, and we assert that

$$|a| \le 2\sqrt{\frac{|C|}{3}} \quad \text{and} \quad |C| \le 2\sqrt{\frac{|B_1C-V_1^2|}{3}} = 2\sqrt{\frac{|a\delta|}{3}}\,.$$

Assume to the contrary first that

$$|a| > 2\sqrt{\frac{|C|}{3}} = 2\sqrt{\frac{|ab_1-u_1^2|}{3}}\,.$$

By Lemma 6.6.3 there exists some $S \in \mathsf{SL}_2(\mathbb{Z})$ such that

$$S\begin{pmatrix} a & u_1 \\ u_1 & b_1\end{pmatrix}S^{\mathsf{t}} = \begin{pmatrix} a' & u' \\ u' & b'\end{pmatrix}, \quad \text{where} \quad |a'| \le 2\sqrt{\frac{|ab_1-u_1^2|}{3}} < |a|\,.$$

We set $\mathbf{0} = (0,0)$ and observe that $a'b' - u'^2 = ab_1 - u_1^2 = C$. Then we obtain

$$T = \begin{pmatrix} S & \mathbf{0}^{\mathsf{t}} \\ \mathbf{0} & 1 \end{pmatrix} \in \mathsf{SL}_3(\mathbb{Z}),$$

$$M_{T\phi_1} = TM_{\phi_1}T^{\mathsf{t}} = \begin{pmatrix} a' & u' & w_1 \\ u' & b' & v_1 \\ w_1 & v_1 & c_1 \end{pmatrix} \quad \text{and} \quad (M_{T\phi_1})^{\#} = \begin{pmatrix} * & * & * \\ * & * & * \\ * & * & C \end{pmatrix}.$$

Since $T\phi_1$ is equivalent to ψ and $|a'| + |C| < |a| + |C|$, this contradicts the minimal choice of $|a| + |C|$.

Assume now that

$$|C| > 2\sqrt{\frac{|a\delta|}{3}}.$$

By **A**, there is some $S_1 \in \mathsf{SL}_2(\mathbb{Z})$ such that

$$S_1 \begin{pmatrix} B_1 & V_1 \\ V_1 & C \end{pmatrix} S_1^{\mathsf{t}} = \begin{pmatrix} B' & V' \\ V' & C' \end{pmatrix}, \quad \text{where} \quad |C'| \le 2\sqrt{\frac{|B_1C - V_1^2|}{3}} < |C|.$$

Now we obtain

$$T_1 = \begin{pmatrix} 1 & \mathbf{0}^{\mathsf{t}} \\ \mathbf{0} & (S_1^{-1})^{\mathsf{t}} \end{pmatrix} \in \mathsf{SL}_3(\mathbb{Z}), \ T_1^{\#} = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0}^{\mathsf{t}} & S_1 \end{pmatrix}, \quad M_{T_1\phi_1} = T_1M_{\phi_1}T_1^{\mathsf{t}} = \begin{pmatrix} a & * & * \\ * & * & * \\ * & * & * \end{pmatrix}$$

and

$$(M_{T_1\phi_1})^{\#} = T_1^{\#}(M_{\phi_1})^{\#}(T_1^{\mathsf{t}})^{\#} = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0}^{\mathsf{t}} & S_1 \end{pmatrix} (M_{\phi_1})^{\#} \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0}^{\mathsf{t}} & S_1^{\mathsf{t}} \end{pmatrix} = \begin{pmatrix} A_1 & U_1 & W_1 \\ U_1 & B' & V' \\ W_1 & V' & C' \end{pmatrix}.$$

Since $T_1\phi_1$ is equivalent to ψ and $|a| + |C'| < |a| + |C|$, this again contradicts the minimal choice of $|a| + |C|$. Thus the inequalities for $|a|$ and $|C|$ are proved.

From

$$|a| \le 2\sqrt{\frac{|C|}{3}} \quad \text{and} \quad |C| \le 2\sqrt{\frac{|a\delta|}{3}} \quad \text{we obtain} \quad a^4 \le \frac{16C^2}{9} \le \frac{64|a\delta|}{27},$$

and therefore

$$|a| \le \frac{4}{3}\sqrt[3]{|\delta|}.$$

Since $C = ab_1 - u_1^2$, it follows that either $aC \ne 0$ or $a = C = u_1 = 0$.

It is now sufficient to prove that there exist α, β, $\gamma \in \mathbb{Z}$ and $\varepsilon \in \{\pm 1\}$ such that the ternary form

$$\phi = \begin{pmatrix} 1 & 0 & 0 \\ \alpha & 1 & 0 \\ \beta & \gamma & 1 \end{pmatrix} \phi_1 = aX^2 + bY^2 + cZ^2 + 2uXY + 2vYZ + 2wXZ$$

has the desired properties. For this, we calculate

$$M_\phi = \begin{pmatrix} 1 & 0 & 0 \\ \alpha & 1 & 0 \\ \beta & \gamma & 1 \end{pmatrix} \begin{pmatrix} a & u_1 & w_1 \\ u_1 & b_1 & v_1 \\ w_1 & v_1 & c_1 \end{pmatrix} \begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & \gamma \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} a & u & w \\ u & b & v \\ w & v & c \end{pmatrix}$$

and

$$(M_\phi)^\# = \begin{pmatrix} 1 & -\alpha & \alpha\gamma-\beta \\ 0 & 1 & -\gamma \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} A_1 & U_1 & W_1 \\ U_1 & B_1 & V_1 \\ W_1 & V_1 & C \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ -\alpha & 1 & 0 \\ \alpha\gamma-\beta & -\gamma & 1 \end{pmatrix} = \begin{pmatrix} A & U & W \\ U & B & V \\ W & V & C \end{pmatrix},$$

where $b = \alpha^2 a + 2\alpha u_1 + b_1$, $c = \beta^2 a + \gamma^2 b_1 + c_1 + 2\beta\gamma u_1 + 2\beta w_1 + 2\gamma v_1$, $u = \alpha a + u_1$, $w = \beta a + \gamma u_1 + w_1$, $v = \alpha\beta a + (\beta + \alpha\gamma) u_1 + \gamma b_1 + \alpha w_1 + v_1$ and $V = V_1 - \gamma C$.

CASE 1: $aC \neq 0$. Assume first that $\alpha,\ \gamma \in \mathbb{Z}$ are such that $-|a| < 2u \le |a|$ and $-|C| < 2|V| \le |C|$. Then there exists some $\beta \in \mathbb{Z}$ such that $-|a| < w \le |a|$.

CASE 2: $a = C = u_1 = 0$. In this case, we obtain $b = b_1$, $u = 0$, $w = w_1$, $c = \gamma^2 b_1 + c_1 + 2\beta w_1 + 2\gamma v_1$, $v = \gamma b_1 + \alpha w_1 + v_1$ and $\delta = -b_1 w_1^2 = -bw^2 \neq 0$. Now we set $e = (2b, 2w)$ and let $k \in \mathbb{Z}$ be such that $-e < 2ke + 4v_1 \le e$. Then there exist $\alpha,\ \gamma \in \mathbb{Z}$ such that $ke = 2w\alpha + 2b\gamma$, and we obtain $-e < 4w\alpha + 4b\gamma + 4v_1 = 4v \le e$. Having chosen α and γ, there exists some $\beta \in \mathbb{Z}$ such that $-|w| < c \le |w|$. □

Exercise 6.6.4. Prove that there are only finitely many equivalence classes of ternary forms of a given determinant.

Theorem 6.6.5. *Let ϕ be a ternary form.*

1. *If $\delta_\phi = -1/4$, then ϕ is equivalent to $Y^2 - XZ$.*
2. *If ϕ is classical and $\delta_\phi = 1$, then ϕ is equivalent to precisely one of the forms*

$$\psi = -Y^2 + 2XZ \quad \text{and} \quad \omega = X^2 + Y^2 + Z^2\,.$$

If in addition $\psi(x, y, z) \ge 0$ for all $(x, y, z) \in \mathbb{Z}^3$, then ϕ is equivalent to ω.

PROOF. We may assume that $\phi = aX^2 + bY^2 + cZ^2 + 2uXY + 2vYZ + 2wXZ$, where $a,\ b,\ c \in \mathbb{Z}$ and $u,\ v,\ w \in \frac{1}{2}\mathbb{Z}$ are such that the inequalities stated in Theorem 6.6.2 hold.

1. Assume that $\delta_\phi = -1/4$. Since

$$\frac{4}{3}\sqrt[3]{\frac{1}{4}} < 1\,, \quad \text{we obtain} \quad a = u = 0 \quad \text{and} \quad -\frac{1}{4} = -bw^2\,, \quad \text{hence} \quad b = 1\,,\ |w| = \frac{1}{2}\,,$$

and therefore $e = (2b, 2w) = 1$. Since $-|w| < c \le |w|$ and $-e < 4v \le e$, it follows that $c = v = 0$. Hence $\phi = Y^2 + 2wXZ = Y^2 \pm XZ$, and since the forms $Y^2 + XZ$ and $Y^2 - XZ$ are equivalent, the assertion follows.

2. Let ϕ be classical and $\delta_\phi = 1$. Then $u,\ v,\ w \in \mathbb{Z}$, $|a| \le 1$, $|C| \le 1$, and therefore either $|a| = 1$ or $a = u = 0$.

CASE 1: $|a| = |C| = 1$. From the inequalities $-|a| < 2u \le |a|$, $2|w| \le |a|$ and $-|C| < 2|V| \le |C|$, it follows that $u = w = V = 0$, hence $V = -av = 0$ and therefore $v = 0$. Since $\delta_\phi = abc = 1$, we obtain $|a| = |b| = |c| = 1$, and (by interchanging the variables) we may assume that $c = 1$ and $a = b \in \{\pm 1\}$. Hence it follows that either $\phi = \omega$ or $\phi = -X^2 - Y^2 + Z^2$.

CASE 2: $a = u = 0$. Then $\delta_\phi = 1 = -bw^2$, hence $|w| = 1$, $b = -1$, $e = 2$, and since $-|w| < c \le |w|$ and $-e < 4v \le e$, we obtain $c \in \{0, 1\}$, $v = 0$, and ϕ is one of the four forms

$$-Y^2 \pm 2XZ \quad \text{and} \quad -Y^2 + Z^2 \pm 2XZ\,.$$

Since the forms $Y^2 + cZ^2 + 2XZ$ and $Y^2 + cZ^2 - 2XZ$ are equivalent, it remains to show that the three forms

$$\psi = -Y^2 + 2XZ\,, \quad \psi_1 = -Y^2 + Z^2 + 2XZ \quad \text{and} \quad \theta = -X^2 - Y^2 + Z^2$$

are equivalent. To prove this, we consider the transformation matrices

$$S = \begin{pmatrix} -1 & -1 & 0 \\ 0 & -1 & -1 \\ 1 & 1 & 1 \end{pmatrix} \quad \text{and} \quad T = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & -1 \\ 1 & 1 & 1 \end{pmatrix} \in \mathsf{SL}_3(\mathbb{Z})\,.$$

It is easily checked that $\theta = S\psi$ and $\psi_1 = T\psi$.

Since ω only represents non-negative integers, while ψ also represents negative integers, these two forms are not equivalent. $\square$

Exercise 6.6.6. Prove that every ternary form of determinant $\frac{1}{2}$ is equivalent to precisely one of the forms $-2Y^2 + XZ$ and $X^2 + Y^2 + Z^2 + XY + XZ + YZ$.

Exercise 6.6.7. Prove that every classical ternary form of determinant 2 is equivalent to precisely one of the forms $X^2 + Y^2 + 2Z^2$, $-X^2 - Y^2 + 2Z^2$ and $2X^2 + 2YZ$.

We proceed with Gauss' proof of the duplication theorem. Let Δ be a quadratic discriminant, and consider the homomorphism $\Psi_\Delta \colon \mathfrak{F}_\Delta \to \text{Ker}(\mathsf{Q}_\Delta)/\mathcal{H}_\Delta$, defined by

$$\Psi_\Delta(F) = \mathcal{H}_F = \{m + \Delta^*\mathbb{Z} \in (\mathbb{Z}/\Delta^*\mathbb{Z})^\times \mid m \in \mathbb{Z},\ (\Delta, m) = 1,\ F \text{ represents } m\}\,.$$

Hence a class $F \in \mathfrak{F}_\Delta$ belongs to $\text{Ker}(\Psi_\Delta)$ if and only if it represents some integer $m \equiv 1 \bmod \Delta^*$. We must prove that $\text{Ker}(\Psi_\Delta) \subset \mathfrak{F}_\Delta^2$. By Theorem 6.4.11, it suffices to prove the following assertion:

G. If $F \in \mathfrak{F}_\Delta$ and F represents some integer $m \equiv 1 \bmod \Delta^*$, then there exists an integer m_0 such that $(\Delta, m_0) = 1$ and F represents m_0^2.

This will be done in the subsequent Theorem 6.6.9. Before however, we need a technical lemma.

Lemma 6.6.8. *Let Δ be a quadratic discriminant, $m_1 \in \mathbb{Z}$ and $(\Delta, m_1) = 1$. If the principal class H_Δ represents some $m \in m_1 + \Delta^*\mathbb{Z}$, then it even represents some $m \in m_1 + \Delta\mathbb{Z}$.*

Proof. We set $\Delta = 4D + \sigma = \varepsilon 2^e P$, where $D \in \mathbb{Z}$, $\sigma \in \{0,1\}$, $\varepsilon = \operatorname{sgn}(\Delta)$, $P = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$, $e, r \in \mathbb{N}_0$, $e_1, \ldots, e_r \in \mathbb{N}$, and $p_1, \ldots, p_r$ are distinct odd primes. Then we obtain $\Delta^* = 2^{c(\Delta)} p_1 \cdot \ldots \cdot p_r$, where

$$c(\Delta) = \begin{cases} 0 & \text{if} \quad \Delta \equiv 1 \mod 4\,, \\ 1 & \text{if} \quad \Delta \equiv 4 \mod 16\,, \\ 2 & \text{if} \quad \Delta \equiv 12 \mod 16 \text{ or } \Delta \equiv 16 \mod 32\,, \\ 3 & \text{if} \quad \Delta \equiv 8 \mod 16 \text{ or } \Delta \equiv 0 \mod 32\,. \end{cases}$$

Suppose that the principal class H_Δ represents an integer $m \in m_1 + \Delta^*\mathbb{Z}$. Then there exist $u, v \in \mathbb{Z}$ such that $m = g_\Delta(u,v) = u^2 + \sigma uv - Dv^2 \equiv m_1 \mod \Delta^*$, and therefore $4m_0 \equiv (2u + \sigma_\Delta v)^2 \mod \Delta^*$. From this, we obtain

$$\Big(\frac{m_0}{p_i}\Big) = \Big(\frac{4m_0}{p_i}\Big) = 1 \quad \text{for all} \quad i \in [1,r]\,,$$

hence m_0 is a quadratic residue modulo P, and there exists some $x_1 \in \mathbb{Z}$ be such that $x_1^2 = g_\Delta(x_1,0) \equiv m_1 \mod P$. If $e = 0$, this implies $m_1 \equiv g_\Delta(x_1,0) \mod \Delta$, and we are done.

Thus suppose that $e \geq 2$. Then $\sigma = 0$, $g_\Delta = [1,0,-D]$, m_1 is odd, and it suffices to prove:

A. There exist $x_0, y_0 \in \mathbb{Z}$ such that $m_1 \equiv x_0^2 - Dy_0^2 \mod 2^e$.

Suppose that **A** holds. Let $x, y \in \mathbb{Z}$ be such that $x \equiv x_1 \mod P$, $x \equiv x_0 \mod 2^e$, $y \equiv 0 \mod P$ and $y \equiv y_0 \mod 2^e$. Then $m = x^2 - Dy^2$ is represented by H_Δ, $m \equiv m_1 \mod 2^e$ and $m \equiv m_1 \mod P$, and therefore $m \equiv m_1 \mod |\Delta|$.

Proof of **A.** Since $m_1 \equiv u^2 - Dv^2 \mod \Delta^*$ implies $m_1 \equiv u^2 - Dv^2 \mod 2^{c(\Delta)}$, there is nothing to do if $e \leq c(\Delta)$. There are three cases with $e > c(\Delta)$.

CASE 1: $\Delta \equiv 4 \mod 16$, $c(\Delta) = 1$, $e = 2$ and $D \equiv 1 \mod 4$. In this case, we set $(x_0, y_0) = (1,0)$ if $m_1 \equiv 1 \mod 4$, and $(x_0,y_0) = (0,1)$ if $m_1 \equiv 3 \mod 4$. Then it obviously follows that $m_1 \equiv x_0^2 - y_0^2 \equiv x_0^2 - Dy_0^2 \mod 4$.

CASE 2: $\Delta \equiv 16 \mod 32$, $c(\Delta) = 2$, $e = 4$ and $D \equiv 4 \mod 8$. It follows that $m_1 \equiv u^2 - Dv^2 \equiv u^2 \equiv 1 \mod 4$, and thus there exists some $y_0 \in \{1,0\}$ such that $m_1 + Dy_0^2 \equiv 1 \mod 8$. Let $x_0 \in \mathbb{Z}$ be such that $x_0^2 \equiv m_1 + Dy_0^2 \mod 16$. Then $m_1 + Dy_0^2$ is a quadratic residue modulo 16, and $m_1 \equiv x_0^2 - Dy_0^2 \mod 16$.

CASE 3: $\Delta \equiv 0 \mod 32$, $c(\Delta) = 3$, $e \geq 5$ and $D \equiv 0 \mod 8$. It follows that $m_1 \equiv u^2 - Dv^2 \equiv u^2 \equiv 1 \mod 8$, and therefore m_1 is a quadratic residue modulo 2^e. Hence there exists some $x_0 \in \mathbb{Z}$ such that $x_0^2 \equiv m_1 \mod 2^e$, and if $y_0 = 0$, then $m_1 \equiv x_0^2 - Dy_0^2 \mod 2^e$. □

Theorem 6.6.9 (Gauss' proof of the duplication theorem). *Let Δ be a quadratic discriminant with associated reduced discriminant Δ^*, $F \in \mathfrak{F}_\Delta$, and assume that F represents some integer $m_1 \equiv 1 \mod \Delta^*$ (hence $F \in \operatorname{Ker}(\Psi_\Delta)$), and $f \in F$. Then there exists a matrix*

$$T = \begin{pmatrix} t & t' & t'' \\ u & u' & u'' \\ * & * & * \end{pmatrix} \in \mathsf{GL}_3(\mathbb{Z})$$

such that $(\Delta, tu' - ut') = 1$,

$$f = (t'X + u'Y)^2 - (tX + uY)(t''X + u''Y) \quad \textit{and} \quad f(-u, t) = (tu' - ut')^2 .$$

In particular, F *represents* $(tu' - ut')^2$ (*which implies* $F \in \mathfrak{F}^2_\Delta$).

PROOF. Suppose that $f = [a, b, c] \in F$. Since $(\Delta, m_1) = 1$, there exists some $n \in \mathbb{Z}$ such that $nm_1 \equiv 1 \bmod \Delta$, and as $n \equiv 1 \bmod \Delta^*$, the principal class H_Δ represents an integer $n_1 \in n + \Delta^*\mathbb{Z}$. By Lemma 6.6.8, H_Δ even represents some $n_1 \in n + \Delta\mathbb{Z}$, and if $m = n_1 m_1$, then $m \equiv nm_1 \equiv 1 \bmod \Delta$, and $F = H_\Delta * F$ represents m. Hence there exist k, l, $n \in \mathbb{Z}$ such that $f(-k, l) + n\Delta = 1$, and we obtain

$$-\frac{1}{4} = -\frac{1}{4}\big[f(-k, l) + n\Delta\big] = \det(A)\,, \quad \text{where} \quad A = \begin{pmatrix} a & b/2 & l/2 \\ b/2 & c & k/2 \\ l/2 & k/2 & n \end{pmatrix} .$$

A is the matrix of the ternary form $\psi = aX^2 + cY^2 + nZ^2 + bXY + lXZ + kYZ$ with determinant $\delta_\psi = \det(A) = -1/4$. By Theorem 6.6.5, ψ is equivalent to the form $\phi = Y^2 - XZ$. Let $T_1 \in \mathsf{GL}_3(\mathbb{Z})$ be such that $T_1 M_\phi T_1^{\mathsf{t}} = A$, and consider the matrix

$$T_1^{\#} = \begin{pmatrix} * & * & * \\ * & * & * \\ r & s & v \end{pmatrix} , \quad \text{where} \quad r,\ s,\ v \in \mathbb{Z}\,.$$

Since $\det(T_1^{\#}) = \det(T_1)^2 = 1$, it follows that $(r, s, v) = 1$, the form $g = [r, -s, v]$ is primitive and thus properly represents some integer coprime with Δ. Let α, $\gamma \in \mathbb{Z}$ be such that $(\alpha, \gamma) = 1$ and $(\Delta, g(\gamma, \alpha)) = 1$, and let β, $\delta \in \mathbb{Z}$ be such that $\alpha\delta - \beta\gamma = 1$. We consider the matrix

$$G = \begin{pmatrix} \alpha^2 & \alpha\beta & \beta^2 \\ 2\alpha\gamma & \alpha\delta + \beta\gamma & 2\beta\delta \\ \gamma^2 & \gamma\delta & \delta^2 \end{pmatrix} \quad \text{and its cofactor matrix} \quad G^{\#} = \begin{pmatrix} * & * & \gamma^2 \\ * & * & -\alpha\gamma \\ * & * & \alpha^2 \end{pmatrix} .$$

A simple (but lengthy) calculation shows that $G \in \mathsf{SL}_3(\mathbb{Z})$ and

$$M_\phi = \begin{pmatrix} 0 & 0 & -1/2 \\ 0 & 1 & 0 \\ -1/2 & 0 & 0 \end{pmatrix} = G M_\phi G^{\mathsf{t}} \,.$$

We set

$$T = T_1 G = \begin{pmatrix} t & t' & t'' \\ u & u' & u'' \\ * & * & * \end{pmatrix} \in \mathsf{GL}_3(\mathbb{Z}) \ \text{ and obtain } \ T^{\#} = T_1^{\#} G^{\#} = \begin{pmatrix} * & * & * \\ * & * & * \\ * & * & g(\gamma, \alpha) \end{pmatrix}$$

and $TMT^{\mathsf{t}} = T_1 G M G^{\mathsf{t}} T^{\mathsf{t}} = A$. Now it follows that

$$f = f(X, Y) = (X\ Y\ 0)\, A \begin{pmatrix} X \\ Y \\ 0 \end{pmatrix} = (X,\, Y,\, 0)\ TMT^{\mathsf{t}} \begin{pmatrix} X \\ Y \\ 0 \end{pmatrix} = \phi\big((X\ Y\ 0)T\big)$$

$$= \phi(tX + uY,\, t'X + u'Y,\, t''X + u''Y) = (t'X + u'Y)^2 - (tX + uY)(t''X + u''Y)\,,$$

$f(-u, t) = (tu' - ut')^2$, $tu' - ut' = g(\gamma, \alpha)$, and $(\Delta, g(\gamma, \alpha)) = 1$. □

6.7. Sums of squares

The representation of a positive integer as a sum of squares (and, more generally, as a sum of k-th powers) of positive integers is a fascinating topic of number theory and attracted a lot of interest through history. We refer to volume II of Dickson's *History of the Theory of Numbers* [**22**] for the development in the past centuries and to [**99**, Ch. XI] for recent work and further references. A recent and extensive presentation of results concerning sums of squares is [**34**].

The representation of an integer as a sum of two squares was already dealt in several places of this volume (Theorems 2.1.7, 3.2.5. 3.4.1, 6.2.6, 6.2.13). We proceed with a necessary and sufficient criterion for the representation of a positive integer as a sum of three squares. This unequally more difficult problem was also solved by Gauss who even proved the following stronger quantitative result:

Let $n \ne 1,\, 3$ *be a positive integer and*

$$\mathsf{r}_3(n) = |\{(x,y,z) \in \mathbb{Z}^3 \mid (x,y,z) = 1,\ x^2+y^2+z^2 = n\}|\,.$$

Then

$$\mathsf{r}_3(n) = \begin{cases} 12h_{-4n} & \textit{if} \quad n \equiv 1 \textit{ or } 2 \mod 4\,, \\ 24h_{-n} & \textit{if} \quad n \equiv 3 \mod 8\,, \\ 0 & \textit{otherwise}\,. \end{cases}$$

We refer to [**104**] for a readable proof of Gauss' quantitative result.

In the sequel we confine ourselves to discussions of the qualitative statement. We shall present two different proofs. The first one, in the spirit of Gauss, makes use of the theory of binary forms and is inspired by [**27**]. The second one, taken from [**34**], avoids the theory of binary form and uses Dirichlet's prime number theorem.

After that, we investigate the (amazingly much simpler) question concerning the representation of positive integers as sums of four and more squares.

We start a preparatory lemma for Gauss' proof of the three-square theorem.

Lemma 6.7.1. *Let* $n,\, a \in \mathbb{N}$ *and* $b,\, c \in \mathbb{Z}$ *be such that* $n = ac - b^2$, $(a,n) = 1$, *and* $-a$ *is a quadratic residue modulo* n. *Then* n *is the sum of three integral squares.*

PROOF. Let $\nu \in \mathbb{Z}$ be such that $-a \equiv \nu^2 \bmod n$. Since $(\nu,n) = 1$, there exists some $\mu \in \mathbb{Z}$ such that $\mu\nu \equiv b \bmod n$, and $-\nu^2 c \equiv ac \equiv b^2 \equiv \mu^2\nu^2 \bmod n$ implies $-c \equiv \mu^2 \bmod n$. Now we define α, β, $\gamma \in \mathbb{Z}$ by

$$\alpha = \frac{c+\mu^2}{n}\,, \quad \beta = \frac{\mu\nu - b}{n}\,, \quad \gamma = \frac{a+\nu^2}{n}\,,$$

and we consider the classical ternary form

$$\psi = \alpha X^2 + \gamma Y^2 + nZ^2 + 2\beta XY + 2\mu XZ + 2\nu YZ \in \mathbb{Z}[X,Y,Z]\,,$$

which represents $n = g(0,0,1)$. Hence it suffices to prove that ψ is equivalent to $\omega = X^2+Y^2+Z^2$. Since

$$M_\psi = \begin{pmatrix} \alpha & \beta & \mu \\ \beta & \gamma & \nu \\ \mu & \nu & n \end{pmatrix}\,, \quad \text{it follows that} \quad M_\psi^\# = \begin{pmatrix} a & b & d \\ b & c & e \\ d & e & s \end{pmatrix}\,,$$

where $d=\beta\nu-\mu\gamma$, $e=\beta\mu-\alpha\nu$ and $s=\alpha\gamma-\beta^2$. We obtain

$$\begin{aligned}\det(M_\psi)&=2\beta\mu\nu+\alpha\gamma n-\alpha\nu^2-\gamma\mu^2-n\beta^2\\&=\frac{1}{n}\Big[2\mu\nu(\mu\nu-b)+(\mu^2+c)(\nu^2+a)\\&\qquad\qquad-(c+\mu^2)\nu^2-(a+\nu^2)\mu^2-(\mu\nu-b)^2\Big]=1\,,\end{aligned}$$

hence $\det(M_\psi^\#)=1$, and we consider the classical ternary form

$$\theta=aX^2+cY^2+sZ^2+2bXY+2dXZ+2eYZ\quad\text{with matrix}\quad M_\theta=M_\psi^\#\,.$$

Since $\delta_\theta=\det(M_\psi^\#)=1$ and

$$\theta(x,y,z)=\frac{1}{a}\Big(ax+by+cz\Big)^2+\frac{1}{an}\Big(ny+(ae-bd)z\Big)^2+\frac{1}{n}\,z^2\geq 0\ \text{ for all }(x,y,z)\in\mathbb{Z}^3,$$

it follows by Theorem 6.6.5 that θ is equivalent to ω. Let $T\in\mathsf{GL}_3(\mathbb{Z})$ be such that $TM_\psi^\#T^{\mathsf t}=M_\omega=I$. As $(M_\psi^\#)^\#=M_\psi$, we obtain $T^\#M_\psi(T^\#)^{\mathsf t}=I=M_\omega$, and therefore ψ is equivalent to ω. □

Theorem 6.7.2 (Gauss' theorem on sums of three squares, basic version). *Every positive integer* $n\not\equiv 0$, 4 *or* 7 mod 8 *is a sum of three integral squares.*

Proof. **1.** (Proof by means of binary forms)

CASE 1: $n\equiv 1$ or 2 mod 4. We consider the quadratic discriminant $\Delta=-4n$. Then $\Delta\equiv 8$ or 12 mod 16, and by Theorem 6.5.13 there exists of some class $F\in\mathfrak{F}_\Delta$ such that $F=[\![a,2b,c]\!]$, where $a\in\mathbb{N}$, $(\Delta,a)=1$ and

$$\Big(\frac{a}{p}\Big)=\Big(\frac{-1}{p}\Big)\quad\text{for all odd primes } p \text{ dividing } n.$$

Hence $-a$ is a quadratic residue modulo n, and n is the sum of three integral squares by Lemma 6.7.1.

CASE 2: $n\equiv 3$ mod 8. We consider the quadratic discriminant $\Delta=-n$. Then $\Delta\equiv 5$ mod 8, $\mathsf{Q}_\Delta(-2)=1$, and by Theorem 6.5.11, there exists some class $F\in\mathfrak{F}_\Delta$ which represents an integer $a_1\in -2+\Delta^*\mathbb{Z}$. Then $a_1=a_0d^2$, where $a_0\in\mathbb{Z}$, $d\in\mathbb{N}$, and F properly represents a_0 (which implies $a_0>0$). Hence we obtain $F=[\![a_0,b,c_0]\!]$ for some b, $c_0\in\mathbb{Z}$. If $a=2a_0$ and $c=2c_0$, then it follows that $-\Delta=n=4a_0c_0-b^2=ac-b^2$. If p is a prime dividing n, then $p\,|\,\Delta^*$, and therefore

$$\Big(\frac{-a}{p}\Big)=\Big(\frac{-2a_1}{p}\Big)=\Big(\frac{4}{p}\Big)=1\,.$$

Consequently, $-a$ is a quadratic residue modulo n, and thus n is the sum of three integral squares. □

2. (Proof by means of Dirichlet's prime number theorem). Let $n\in\mathbb{N}$ be such that $n\not\equiv 0$, 4, 7 mod 8. It suffices to prove the following assertion:

A. There exist integers a, b, u such that $D=ab-u^2>0$ and $nD-b=1$.

Suppose that **A** holds. We consider the classical ternary form

$$\psi = aX^2 + bY^2 + nZ^2 + 2uXY + 2XZ \quad \text{and its matrix} \quad M_\psi = \begin{pmatrix} a & u & 1 \\ u & b & 0 \\ 1 & 0 & n \end{pmatrix}.$$

Then $\psi(0,0,1) = n$, and therefore it suffices to prove that ψ is equivalent to the form $\omega = X^2 + Y^2 + Z^2$. We use Theorem 6.6.5. By assumption, $\det(\psi) = nD - b = 1$, and for all $(x,y,z) \in \mathbb{Z}^3$ we obtain

$$a\psi(x,y,z) = (ax + uy + nz)^2 + Dy^2 - 2uyz + (an-1)z^2.$$

Since $b = nD - 1 \ge 2D - 1 > 0$ and $ab = D + u^2 \ge D > 0$, it follows that $a > 0$, and since $u^2 - D(an-1) = a(b - Dn) = -a < 0$, the form $DY^2 - 2uYZ + (an-1)Z^2$ is positive definite. Hence we obtain $\psi(x,y,z) \ge 0$ for all $(x,y,z) \in \mathbb{Z}^3$, and we are done.

Proof of **A.** We use Dirichlet's prime number theorem.

CASE 1: $n \equiv 2 \mod 4$. Since $(4n, n-1) = 1$, there exists some $m \in \mathbb{N}$ such that $b = n - 1 + 4mn$ is a prime. If $D = 4m + 1$, then $b = Dn - 1$, and

$$\Big(\frac{-D}{b}\Big) = \Big(\frac{b}{D}\Big) = \Big(\frac{-1}{D}\Big) = 1.$$

Hence $-D$ is a quadratic residue modulo b, and therefore $-D = u^2 - ab$ for some $a,\, u \in \mathbb{Z}$.

CASE 2: $n \equiv 1 \mod 2$. We set

$$c = \begin{cases} 1 & \text{if} \quad n \equiv 3 \mod 4, \\ 3 & \text{if} \quad n \equiv 1 \mod 4, \end{cases} \qquad \text{and} \quad cn - 1 = 2u, \quad \text{where } u \in \mathbb{N} \text{ is odd.}$$

Since $(4n, u) = 1$, there exists some $m \in \mathbb{N}$ such that $u + 4mn$ is a prime. We set $D = 8m + c$ and $b = Dn - 1 = 2p$. Then we obtain the following values:

n mod 8	D mod 8	Dn mod 8	p mod 4
1	3	3	1
3	1	3	1
5	3	7	3

In each case, we calculate

$$\Big(\frac{-D}{p}\Big) = \Big(\frac{p}{D}\Big) = \Big(\frac{-2p}{D}\Big)\Big(\frac{-2}{D}\Big) = 1.$$

Hence $-D$ is a quadratic residue modulo b, and therefore $-D = u^2 - ab$ for some $a,\, u \in \mathbb{Z}$. □

Theorem 6.7.3 (Gauss' theorem on sums of three squares, full version)**.**
A positive integer m is a sum of three integral squares if and only if m is not of the form $m = 4^e(8k+7)$ for some $e,\, k \in \mathbb{N}_0$.

PROOF. We proceed by induction on e.

$e = 0$: If m is a sum of three integral squares, then $m = x_1^2 + x_2^2 + x_3^2$, where $x_i \in \mathbb{N}$, hence $x_i^2 \equiv 0$, 1 or 4 mod 8 for all $i \in [1,3]$, and therefore $m \not\equiv 7 \mod 8$.

Conversely, if $m \not\equiv 7 \bmod 8$, then m is a sum of three integral squares by Theorem 6.7.2.

$e \geq 1\,,\ e-1 \to e$: If $e \geq 1$ and $4^e n = x_1^2 + x_2^2 + x_3^2$, where $x_i \in \mathbb{N}$, then it follows that $x_i \equiv 0 \bmod 2$ for all $i \in [1,3]$. Hence $4^e n$ is a sum of three integral squares if and only if $4^{e-1}n$ is a sum of three integral squares, and the assertion follows by the induction hypothesis. ☐

Exercise 6.7.4. An integer of the form $n(n+1)/2$ for some $n \in \mathbb{N}_0$ is called a *triangular number*. Prove that every positive integer is the sum of three triangular numbers.

Exercise 6.7.5. Prove that a positive integer is a sum of three rational squares if and only if it is a sum of three integral squares. Deduce that there are no rational numbers x, y, z such that $x^2 + y^2 + z^2 + x + y + z = 1$.

The following theorem of Lagrange on sums of four squares follows immediately from Theorem 6.7.3. It is however so much more elementary that we shall also give a direct proof.

Theorem 6.7.6 (Lagrange's theorem on sums of four squares)**.** *Every positive integer is a sum of four integral squares.*

Proof. **1.** (Proof by means of Gauss' theorem on sums of three squares). Suppose that $m = 4^k m_0$, where $k \in \mathbb{N}_0$, $m_0 \in \mathbb{N}$ and $4 \nmid m_0$. We set $e = 1$ if $m_0 \equiv 7 \bmod 8$, and $e = 0$ otherwise. Then there exist $x_1,\, x_2,\, x_3 \in \mathbb{N}_0$ such that $m_0 - e = x_1^2 + x_2^2 + x_3^2$, and therefore $m = (2^k x_1)^2 + (2^k x_2)^2 + (2^k x_3)^2 + (2^k e)^2$. ☐

2. (Elementary proof) We make use of the following identity, valid for elements of any commutative ring.

$$\begin{aligned}(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) = \quad & (a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4)^2 \\ & + (a_1b_2 - a_2b_1 + a_3b_4 - a_4b_3)^2 \\ & + (a_1b_3 - a_3b_1 + a_2b_4 - a_4b_2)^2 \\ & + (a_1b_4 - a_4b_1 + a_2b_3 - a_3b_2)^2\,.\end{aligned}$$

This identity shows that the set $L = \{a_1^2 + a_2^2 + a_3^2 + a_4^2 \mid a_1,\, a_2,\, a_3,\, a_4 \in \mathbb{Z}\}$ is multiplicatively closed, and therefore it suffices to prove that every prime p is a sum of four integral squares. Since $2 = 1^2 + 1^2 + 0^2 + 0^2$, we may assume that $p > 2$.

If $p = 2N+1$ and $i,\, j \in [0,N]$, then $i \neq j$ implies $i^2 \not\equiv j^2 \bmod p$. Hence

$$|\{1 + j^2 \mid j \in [0,N]\,\}| = |\{-j^2 \mid j \in [0,N]\,\}| = N+1\,,$$

and as $2(N+1) = p+1$, there exist $x,\, y \in [0, N+1] \subset [0, p-1]$ such that

$$1 + x^2 + y^2 + 0^2 = pn \quad \text{for some} \quad n \in \mathbb{N}\,.$$

In particular, there exists some $n \in \mathbb{N}$ such that np is the sum of four integral squares which are not all divisible by p. Let $n \in \mathbb{N}$ be minimal with this property, and set $np = x_1^2 + x_2^2 + x_3^2 + x_4^2$, where $x_1,\, x_2,\, x_3,\, x_4 \in \mathbb{Z}$ and $p \nmid x_i$ for some $i \in [1,4]$. We must prove that $n = 1$. First we show:

A. n is odd and $n < p$.

Proof of **A.** If n is even, then we may (after renumbering if necessary) assume that $x_1 \equiv x_2 \mod 2$ and $x_3 \equiv x_4 \mod 2$, and we obtain

$$\frac{n}{2}\,p = \Bigl(\frac{x_1-x_2}{2}\Bigr)^2 + \Bigl(\frac{x_1+x_2}{2}\Bigr)^2 + \Bigl(\frac{x_3-x_4}{2}\Bigr)^2 + \Bigl(\frac{x_3+x_4}{2}\Bigr)^2 ,$$

and this contradicts the minimal choice of n. Hence n is odd. For $i \in [1,4]$, let $y_i \in [-N,N]$ be such that $y_i \equiv x_i \bmod p$. Then $y_i \neq 0$ for some $i \in [1,4]$, and $y_1^2+y_2^2+y_3^2+y_4^2 \equiv x_1^2+x_2^2+x_3^2+x_4^2 \equiv 0 \mod p$, say $y_1^2+y_2^2+y_3^2+y_4^2 = mp$ for some $m \in \mathbb{N}$. By the minimal choice of n we obtain $np \le mp = y_1^2+y_2^2+y_3^2+y_4^2 < 4N^2 < p^2$ and thus $n < p$. $\square$[**A.**]

Let now z_1, z_2, z_3, $z_4 \in \mathbb{Z}$ be such that

$$|z_i| < \frac{n}{2} \quad \text{and} \quad z_i \equiv x_i \mod n \quad \text{for all} \quad i \in [1,4] .$$

If $z_i = 0$ for all $i \in [1,4]$, then $x_i \equiv 0 \mod n$ for all $i \in [1,4]$, and $np \equiv 0 \mod n^2$. Since $n < p$, this implies $n = 1$, and we are done.

Thus suppose that $z_i \neq 0$ for some $i \in [1,4]$. Since

$$z_1^2 + z_2^2 + z_3^2 + z_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \mod n ,$$

there is some $l \in \mathbb{N}$ such that $nl = z_1^2 + z_2^2 + z_3^2 + z_4^2 < n^2$, hence $l < n$, and we obtain

$$n^2lp = (np)(nl) = (x_1^2+x_2^2+x_3^2+x_4^2)(z_1^2+z_2^2+z_3^2+z_4^2) = u_1^2+u_2^2+u_3^2+u_4^2 ,$$

where

$$\begin{aligned}
u_1 &= x_1z_1 + x_2z_2 + x_3z_3 + x_4z_4 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \mod n ,\\
u_2 &= x_1z_2 - x_2z_1 + x_3z_4 - x_4z_3 \equiv x_1x_2 - x_2x_1 + x_3x_4 - x_4x_3 \equiv 0 \mod n ,\\
u_3 &= x_1z_3 - x_3z_1 + x_2z_4 - x_4z_2 \equiv x_1x_3 - x_3x_1 + x_2x_4 - x_xz_2 \equiv 0 \mod n ,\\
u_4 &= x_1z_4 - x_4z_1 + x_2z_3 - x_3z_2 \equiv x_1x_4 - x_4x_1 + x_2x_3 - x_3x_2 \equiv 0 \mod n .
\end{aligned}$$

For $i \in [1,4]$, let $t_i \in \mathbb{Z}$ be such that $u_i = nt_i$. Then $n^2lp = n^2(t_1^2+t_2^2+t_3^2+t_4^2)$, hence lp is the sum of four integral squares, but $l < n$, a contradiction. $\square$

Exercise 6.7.7. Let n be a positive integer. Prove that $8n$ is a sum of eight and not fewer positive integral squares.

Exercise 6.7.8. Suppose that $d \in [1,7]$. Prove that every positive integer n has a representation $n = x_1^2 + x_2^2 + x_3^2 + dx_4^2$, where x_1, x_2, x_3, x_4 are integers.

Theorem 6.7.9 (Jacobi)**.** *Every positive integer n has a representation*

$$n = a^2 + 2b^2 + 3c^2 + 6d^2 , \quad \textit{where} \quad a,\ b,\ c,\ d \quad \textit{are integers.}$$

Proof. Let n be a positive integer. We show first:

A. There exist integers a, b, c, d such that $n = a^2+b^2+c^2+d^2$ and $3 \mid a+b+c$.

Proof of **A.** By Theorem 6.7.6, there exist integers x_1, x_2, x_3, x_4 such that $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Let $r = |\{i \in [1,4] \mid x_i \equiv 0 \bmod 3\}|$. If $r \geq 3$, we are done.

If $r = 2$, we may assume that $x_3 \equiv x_4 \equiv 0 \bmod 3$, and $x_1 \equiv \varepsilon x_2 \equiv 1 \bmod 3$ for some $\varepsilon \in \{\pm 1\}$. Then $(a,b,c,d) = (x_1, -\varepsilon x_2, x_3, x_4)$ satisfies our requirements.

If $r \leq 1$, we may assume that $x_1 \equiv \varepsilon x_2 \equiv \eta x_3 \bmod 3$ for some ε, $\eta \in \{\pm 1\}$, and then $(a,b,c,d) = (x_1, \varepsilon x_2, \eta x_3, x_4)$ satisfies our requirements. $\square$[**A.**]

Assume now that $n = a^2 + b^2 + c^2 + d^2$, where a, b, c, d are integers such that $a + b + c = 3z$ for some $z \in \mathbb{Z}$. We may assume that $a \equiv b \bmod 2$, and therefore $a + b - 2c = a + b - (6z - 2a - 2b) \equiv 3a + 3b \equiv 0 \bmod 6$. We set $a + b - 2c = 6t$ and $a - b = 2y$, where t, $y \in \mathbb{Z}$, and we obtain

$$3(a^2 + b^2 + c^2) = (a + b + c)^2 + 2\Big(\frac{a+b}{2} - c\Big)^2 + 6\Big(\frac{a-b}{2}\Big)^2 = 9z^2 + 18t^2 + 6y^2\,.$$

Hence it follows that $n = a^2 + b^2 + c^2 + d^2 = d^2 + 2y^2 + 3z^2 + 6t^2$. $\square$

Jacobi's Theorem 6.7.9 fits into a more general theory as follows. Call a quadruple (A, B, C, D) of positive integers such that $A \leq B \leq C \leq D$ *universal* if every positive integer n is of the form $n = Aa^2 + Bb^2 + Cc^2 + Dd^2$, where a, b, c, d are integers. There exist 54 universal quadruples:

$(1,1,1,D)$ where $D \in [1,7]$; $(1,1,2,D)$ where $D \in [2,14]$;
$(1,1,3,D)$ where $D \in [3,6]$; $(1,2,2,D)$ where $D \in [2,7]$;
$(1,2,3,D)$ where $D \in [3,10]$; $(1,2,4,D)$ where $D \in [4,14]$;
$(1,2,5,D)$ where $D \in [6,10]$.

For details and a wealth of similar elementary results we refer to [**21**].

A substantially more general result is given by the 15-Theorem of Conway and Schneeberger and the 290-Theorem of Bhargava and Hanke (see [**7**] and the notes by Y. S. Moon in http://math.stanford.edu/theses/moon.pdf). These theorems deal with integral quadratic forms in $n \geq 4$ variables, given by

$$f(X_1, \ldots, X_n) = \sum_{1 \leq i \leq j \leq n} a_{i,j} X_i X_j \in \mathbb{Z}[X_1, \ldots, X_n]\,.$$

In accordance with our terminology for ternary forms, we call such a form *classical* if $a_{i,j} \equiv 0 \bmod 2$ whenever $i < j$, and we call it positive definite if $f(\boldsymbol{x}) > 0$ for all $\boldsymbol{0} \neq \boldsymbol{x} \in \mathbb{Z}^n$. Then the following assertions hold:

15-Theorem. *If a classical integral positive definite quadratic form represents the numbers* 1, 2, 3, 5, 6, 7, 10, 14 *and* 15*, then it represents all positive integers.*

290-Theorem. *If an integral positive definite quadratic form represents the numbers* 1, 2, 3, 5, 6, 7, 10, 13, 14, 15, 17, 19, 21, 22, 23, 26, 29, 30, 31, 34, 35, 37, 42, 58, 93, 110, 145, 203 *and* 290*, then it represents all positive integers.*

We close this section with a refinement of Lagrange's theorem on sums of four squares. We suppose that $k \geq 4$ and investigate which positive integers are sums of k positive squares. These and related questions are dealt with in [**34**, Ch. 6], [**87**], [**35**] and [**5**].

Theorem 6.7.10. *For $k \in \mathbb{N}$, let Q_k be the set of all $n \in \mathbb{N}$ which are not a sum of k positive integral squares.*

1. $Q_4 = \{1,\, 3,\, 5,\, 9,\, 11,\, 17,\, 29,\, 41\} \cup \{\, 4^a{\cdot}2\,,\ 4^a{\cdot}6\,,\ 4^a{\cdot}14 \mid a \in \mathbb{N}_0\}$.
2. $Q_5 = \{1,\, 2,\, 3,\, 4,\, 6,\, 7,\, 9,\, 10,\, 12,\, 15,\, 18,\, 33\}$.
3. *If $k \geq 6$, then*

$$Q_k = [1, k-1] \cup \{k + b \mid b \in B\}\,, \quad \textit{where} \quad B = \{1,\, 2,\, 4,\, 5,\, 7,\, 10,\, 13\}\,.$$

Proof. 1. Let $n \in \mathbb{N}$.

CASE 1: $8 \nmid n$, $n \leq 169$ if $n \not\equiv 1 \bmod 4$, and $n \leq 676$ if $n \equiv 1 \bmod 4$. A tedious but simple calculation shows that $n \in Q_4$ if and only if

$$n \in \{1,\, 2,\, 3,\, 5,\, 6,\, 9,\, 11,\, 14,\, 17,\, 29,\, 41\}\,.$$

CASE 2: $8 \nmid n$, $n \not\equiv 1 \bmod 4$, and $n \geq 170$. As $n - 169 \not\equiv 0$, 4 or $7 \bmod 8$, Theorem 6.7.3 implies that $n - 169$ is a sum of three squares, say $n = a^2 + b^2 + c^2$, where $a,\, b,\, c \in \mathbb{N}_0$ and $a \geq b \geq c$. Now we obtain

$$n = \begin{cases} 13^2 + a^2 + b^2 + c^2 & \text{if} \quad c > 0\,, \\ 5^2 + 12^2 + a^2 + b^2 & \text{if} \quad b > 0 = c\,, \\ 3^2 + 4^2 + 5^2 + a^2 & \text{if} \quad b = 0\,, \end{cases}$$

and therefore $n \notin Q_4$.

CASE 3: $8 \nmid n$, $n \equiv 1 \bmod 4$, and $n \geq 677$. Then $n - 676 \equiv 1 \bmod 4$, and Theorem 6.7.3 implies that $n - 676$ is a sum of three squares, say $n = a^2 + b^2 + c^2$, where $a,\, b,\, c \in \mathbb{N}_0$ and $a \geq b \geq c$. Now we obtain

$$n = \begin{cases} 26^2 + a^2 + b^2 + c^2 & \text{if} \quad c > 0\,, \\ 10^2 + 24^2 + a^2 + b^2 & \text{if} \quad b > 0 = c\,, \\ 6^2 + 8^2 + 10^2 + a^2 & \text{if} \quad b = 0\,, \end{cases}$$

and therefore $n \notin Q_4$.

CASE 4: $n = 4^a m$, where $a,\, m \in \mathbb{N}$, $a \geq 2$ and $2 \nmid m$. In this case, we obtain $n = 4^{a-1}(4m)$ and $4m \equiv 4 \bmod 8$. By the CASES 1, 2 and 3, it follows that that $4m \notin Q_4$. If $4m = x_1^2 + x_2^2 + x_3^2 + x_4^2$, where $x_1,\, x_2,\, x_3,\, x_4 \in \mathbb{N}$, then $n = (2^{a-1}x_1)^2 + (2^{a-1}x_2)^2 + (2^{a-1}x_3)^2 + (2^{a-1}x_4)^2$, and therefore $n \notin Q_4$.

CASE 5: $n = 4^a m$, where $a,\, m \in \mathbb{N}$ and $m \equiv 2 \bmod 4$. We assert that $n \notin Q_4$ if and only if $m \notin Q_4$. Then it follows from the CASES 1, 2 and 3 that $n \in Q_4$ if and only if $m \in \{2,\, 6,\, 14\}$.

If $m \notin Q_4$ and $x_1,\, x_2,\, x_3,\, x_4 \in \mathbb{N}$ are such that $m = x_1^2 + x_2^2 + x_3^2 + x_4^2$, then $n = (2^a x_1)^2 + (2^a x_2)^2 + (2^a x_3)^2 + (2^a x_4)^2 \notin Q_4$.

As to the converse, suppose that $n \notin Q_4$, and let $b \in [0, a]$ be minimal such that $4^b m \notin Q_4$. If $b \geq 1$, then $8 \,|\, 4^m b$, and if $4^b m = x_1^2 + x_2^2 + x_3^2 + x_4^2$, where $x_1,\, x_2,\, x_3,\, x_4 \in \mathbb{N}$, then $2 \,|\, x_i$, hence $x_i = 2y_i$, where $y_i \in \mathbb{N}$ for all $i \in [1, 4]$, and $4^{b-1}m = y_1^2 + y_2^2 + y_3^2 + y_4^2$, contradicting the minimal choice of b. Hence $b = 0$ and $m \notin Q_4$.

2. We use 1. If $n \in Q_5$ and $n \geq 1$, then $n - 1 \in Q_4$, and therefore

$$Q_5 \subset \{1,\, 2,\, 4,\, 6,\, 10,\, 12,\, 18,\, 30,\, 42\} \cup \{\, 4^a{\cdot}2 + 1\,,\ 4^a{\cdot}6 + 1\,,\ 4^a{\cdot}14 + 1 \mid a \in \mathbb{N}_0\}\,.$$

Obviously, $\{3,\,7,\,9,\,15\}\subset Q_5$. If $N=4^ak+1\in Q_5$ for some $a,\,k\in\mathbb{N}$ such that $2\,|\,k$, then $n-4\in Q_4$, and as $n-4\equiv 5 \bmod 8$, it follows that $n-4\in\{5,\,29\}$, and it is easily checked that $\{9,\,33\}\subset Q_5$. Since $30=3^2+3^2+2^2+2^2+2^2\notin Q_5$ and $42=4^2+3^2+3^2+2^2+2^2\notin Q_5$, the assertion follows.

3. We use 2. Suppose that $k\ge 6$. It is obvious that $[1,k-1]\subset Q_k$ and $k\notin Q_k$. If $n\in Q_k$ and $n>k$, then $n-k+5\in Q_5$, and therefore $n=k+b$, where $b\in\{1,\,2,\,4,\,5,\,7,\,10,\,13,\,28\,\}$. Since $k+28=(k-4)1^2+5^2+2^2+1^2+1^2+1^2\notin Q_k$, it remains to prove:

$$\text{If } n\in[k,\,k+13]\setminus Q_k, \text{ then } n=k+b, \text{ where } b\in\{0,\,3,\,6,\,8,\,9,\,11,\,12\,\}.$$

For $\boldsymbol{x}=(x_1,\ldots,x_k)\in\mathbb{N}^k$ with $x_1\le x_2\le\ldots\le x_k$, we set $s(\boldsymbol{x})=x_1^2+\ldots+x_k^2$. Then $s(\boldsymbol{x})\le k+13$ is only achieved by the following seven possibilities:

$$\boldsymbol{x}=(1,\ldots,1,\,1)\,,\;\; s(\boldsymbol{x})=k\,;\quad \boldsymbol{x}=(1,\ldots,1,2)\,,\;\; s(\boldsymbol{x})=k+3\,;$$
$$\boldsymbol{x}=(1,\ldots,1,3)\,,\;\; s(\boldsymbol{x})=k+8\,;\quad \boldsymbol{x}=(1,\ldots,1,2,2)\,,\;\; s(\boldsymbol{x})=k+6\,;$$
$$\boldsymbol{x}=(1,\ldots,1,2,3)\,,\;\; s(\boldsymbol{x})=k+11\,;\quad \boldsymbol{x}=(1,\ldots,1,2,2,2)\,,\;\; s(\boldsymbol{x})=k+9\,;$$
$$\boldsymbol{x}=(1,\ldots,1,2,2,2,2)\,,\;\; s(\boldsymbol{x})=k+12\,.$$

□

This page intentionally left blank

CHAPTER 7

Cubic and biquadratic residues

In Chapter 3, we started with some elementary facts concerning power residues, and then we proceeded with quadratic residues, quadratic reciprocity and its consequences. To obtain a similar theory including reciprocity laws for higher power residues, one has to leave the rational number field. Already Gauss noticed that in order to formulate a reciprocity law for cubic or biquadratic residues it is necessary to use complex integers, but it was only Eisenstein who gave complete proofs for the biquadratic and cubic reciprocity laws using the cyclotomic fields of fourth and third roots of unity. Moreover, he succeeded in proving a special case of the general reciprocity law for l-th power residues, where l is an odd prime. Only class field theory, as developed by Takagi, Hasse and Artin, provided a full insight into higher reciprocity laws. Here we must limit ourselves to these sketchy remarks, for a full history of the subject and more details we refer to Lemmermeyer's book [**67**].

In this chapter we present the theory of cubic and biquadratic residues and reciprocity laws. We start with the cubic reciprocity law in the integral domain $E = \mathbb{Z}[\rho]$ (where $\rho = \zeta_3 = \mathsf{e}^{2\pi \mathsf{i}/3}$) and the biquadratic reciprocity law in the integral domain $D = \mathbb{Z}[\mathsf{i}]$. Our main references for these reciprocity laws are [**44**] and [**67**]. After that, we continue with a detailed discussion of rational biquadratic reciprocity laws, and we close with a presentation of Z.-H. Sun's explicit construction of a biquadratic class group character and its consequences.

Throughout this chapter, we shall tacitly use the results of Chapter 3 (in particular, Gauss and Jacobi sums and the properties of the Legendre and Jacobi symbols) without further reference.

7.1. The cubic Jacobi symbol

Throughout this and the following sections, let $\rho = \zeta_3 = (-1+\sqrt{-3}\,)/2$ *be the normalized primitive* 3*rd root of unity, and* $E = \mathbb{Z}[\rho]$.

We start with some elementary results concerning the arithmetic of E and its quotient field $K = \mathsf{q}(E) = \mathbb{Q}(\rho) = \mathbb{Q}(\sqrt{-3}\,)$. Recall that K is a quadratic number field with discriminant $\Delta_K = -3$ (Theorem 1.1.9), $E = \mathcal{O}_{-3} = \mathcal{O}_K$ is its ring of integers (Definition 5.1.6), $-\rho = \zeta_6^{-1}$, $\overline{\rho} = \rho^2 = \rho^{-1}$, $E^\times = \langle -\rho \rangle$ (Theorem 5.2.1.1), and $\omega_{-3} = \rho$ is the basis number of discriminant -3. Every $z \in K$ has a unique representation $z = a + b\rho$, where $a,\, b \in \mathbb{Q}$, and then

$$\mathcal{N}(z) = (a+b\rho)(a+b\rho^2) = a^2 - ab + b^2\,.$$

Since $h_K = h_{-3} = 1$, it follows that E is a principal ideal domain (Theorem 5.8.6).

For every prime element $\pi \in E$, there is a unique prime $p \in \pi E$, we have $\pi E \cap \mathbb{Z} = p\mathbb{Z}$, $E/\pi E$ is a field, and $|E/\pi E| = \mathfrak{N}_{-3}(\pi E) = \mathcal{N}(\pi)$ (Theorem 5.8.1 and Definition 5.4.1). In particular,

$$(E/\pi E)^\times = \{\alpha + \pi E \mid \alpha \in E \setminus \pi E\}$$

is a cyclic group of order $\mathcal{N}(\pi) - 1$, and the inclusion $\mathbb{Z} \hookrightarrow E$ induces a monomorphism $\iota_\pi \colon \mathbb{F}_p \to E/\pi E$, given by $\iota_\pi(a+p\mathbb{Z}) = a+\pi E$ for all $a \in \mathbb{Z}$. Throughout, we shall identify $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ with its image under ι_π, and then $a+p\mathbb{Z} = a+\pi E \in E/\pi E$ for all $a \in \mathbb{Z}$.

Conversely, if p is a prime, then Theorem 5.8.8 implies that p behaves in E as follows:

1. If $p \equiv 2 \mod 3$, then p is a prime element of E, and $\mathcal{N}(p) = p^2$.
2. If $p \equiv 1 \mod 3$, then there exist $a,\, b \in \mathbb{N}$ such that the elements $\pi = a + b\rho$ and $\overline{\pi} = a + b\rho^2$ are prime elements of E,
$$\mathcal{N}(\pi) = \mathcal{N}(\overline{\pi}) = \pi\overline{\pi} = p = a^2 - ab + b^2\,,$$
$E/\pi E = \{a + \pi E \mid a \in \mathbb{Z} \setminus p\mathbb{Z}\}$ and $E/\overline{\pi} E = \{a + \overline{\pi} E \mid a \in \mathbb{Z} \setminus p\mathbb{Z}\}$. If $\alpha,\, \beta \in E$, then $\alpha \equiv \beta \mod \pi$ if and only if $\overline{\alpha} \equiv \overline{\beta} \mod \overline{\pi}$, and $(\alpha, \pi) = 1$ if and only if $(\overline{\alpha}, \overline{\pi}) = 1$. In particular, if $a,\, b \in \mathbb{Z}$, then $a \equiv b \mod \pi$ if and only if $a \equiv b \mod p$, and $(a, \pi) = 1$ if and only $p \nmid a$.
3. $\sqrt{-3} = \rho(1-\rho)$ is a prime element of E, and $\mathcal{N}(\sqrt{-3}\,) = 3$. In particular, for $\alpha \in E$ the following assertions are equivalent:
$$\textbf{a)}\ (\alpha, 3) = 1; \quad \textbf{b)}\ \alpha \notin \sqrt{-3}\,E; \quad \textbf{c)}\ 3 \nmid \mathcal{N}(\alpha).$$

Consequently, if $\pi \in E \setminus \sqrt{-3}\,E$ is a prime element, then

- either $\mathcal{N}(\pi) = p \equiv 1 \mod 3$ is a prime, and $E/\pi E = \mathbb{F}_p$,
- or $\pi E = pE$ for some prime $p \equiv 2 \mod 3$, and $E/\pi E = E/pE$ is a field with p^2 elements.

In both cases, it follows that $|(E/\pi E)^\times| \equiv 0 \mod 3$, and since the 3 residue classes $1 + \pi E$, $\rho + \pi E$, $\rho^2 + \pi E$ are distinct, we obtain $\operatorname{ord}(\rho + \pi E) = 3$, and

$$\{\xi \in E/\pi E \mid \xi^3 = 1 + \pi E\} = \{\rho^k + \pi E \mid k \in [0, 2]\,\} = \langle \rho + \pi E\rangle\,.$$

Since $|E^\times| = 6$, every $\alpha \in D^\bullet$ has 6 associates, but the following elementary Lemma 7.1.1 allows us to single out one of them. If $\alpha = a + b\rho \in E$, where $a,\, b \in \mathbb{Z}$, then $\alpha \equiv 1 \mod 3$ (in E) if and only if $a \equiv 1 \mod 3$ and $b \equiv 0 \mod 3$.

Lemma 7.1.1.

1. *The map* $E^\times \to (E/3E)^\times$, *defined by* $\varepsilon \mapsto \varepsilon + 3E$, *is an isomorphism. In particular,* $(E/3E)^\times = \langle -\rho + 3E\rangle = \{\varepsilon + 3E \mid \varepsilon \in E^\times\}$, *and if* $\varepsilon,\, \varepsilon_1 \in E^\times$, *then* $\varepsilon \equiv \varepsilon_1 \mod 3$ *implies* $\varepsilon = \varepsilon_1$.
2. *If* $\alpha,\, \beta \in E \setminus \sqrt{-3}\,E$ *are such that* $\alpha \equiv \beta \mod 3$ *and* $\alpha E = \beta E$, *then* $\alpha = \beta$.
3. *For every* $\alpha \in E \setminus \sqrt{-3}\,E$, *there is a unique* $\varepsilon \in E^\times$ *such that* $\alpha\varepsilon \equiv 1 \mod 3$.
4. *Let* $p \equiv 1 \mod 3$ *be a prime. Then there exists a prime element* $\pi \in E$ *such that* $\pi \equiv 1 \mod 3$ *and* $\mathcal{N}(\pi) = p$. *If* $\pi_1 \in E$ *is another prime element such that* $\pi_1 \equiv 1 \mod 3$ *and* $\mathcal{N}(\pi_1) = p$, *then* $\pi_1 \in \{\pi, \overline{\pi}\}$.

Proof. 1. If $k,\,j \in [0,5]$ and $k<j$, then

$$(-\rho)^j - (-\rho)^k = (-\rho)^k[(-\rho)^{j-k}-1] \not\equiv 0 \mod 3\,.$$

Hence the six residue classes $\{(-\rho)^j + 3E \mid j \in [0,5]\} \subset (E/3E)^\times$ are distinct, and since $|(E/3E)^\times| = 6$ (by Theorem 5.9.3), the assertion follows.

2. If $\alpha E = \beta E$, then $\beta = \alpha\varepsilon$ for some $\varepsilon \in E^\times$, and $\alpha \equiv \beta \equiv \alpha\varepsilon \mod 3$ implies $\varepsilon \equiv 1 \mod 3$ and thus $\varepsilon = 1$.

3. If $\alpha \in E \setminus \sqrt{-3}\,E$, then $\alpha + 3E \in (E/3E)^\times$. Hence there exists some $\varepsilon \in E^\times$ such that $\alpha \equiv \varepsilon^{-1} \mod 3$, and consequently $\alpha\varepsilon \equiv 1 \mod 3$. The uniqueness follows by 2.

4. If $p \equiv 1 \mod 3$, then $p = \pi_0\overline{\pi}_0$ for some prime element $\pi_0 \in E$, and by 3. there exists some $\varepsilon \in E^\times$ such that $\pi = \pi_0\varepsilon \equiv 1 \mod 3$. Then π is a prime element of E, $\overline{\pi} \equiv 1 \mod 3$, and $p = \pi\overline{\pi}$. Let $\pi_1 \in E$ be another prime element such that $p = \pi_1\overline{\pi}_1$ and $\pi_1 \equiv 1 \mod 3$. By unique factorization, we get either $\pi_1 = \varepsilon\pi$ or $\pi_1 = \varepsilon\overline{\pi}$ for some $\varepsilon \in E^\times$ and thus either $\pi_1 = \pi$ or $\pi_1 = \overline{\pi}$. □

Exercise 7.1.2. Prove that every $\alpha \in E^\bullet$ has an (up to the order of the factors) unique factorization $\alpha = \varepsilon(\sqrt{-3}\,)^e\pi_1 \cdot \ldots \cdot \pi_r$, where $\varepsilon \in E^\times$, $e \in \mathbb{N}_0$, $r \in \mathbb{N}_0$ and $\pi_1, \ldots, \pi_r$ are prime elements of E satisfying $\pi_i \equiv 1 \mod 3$ for all $i \in [1,r]$

As a first consequence of Lemma 7.1.1, we investigate the various representations of primes $p \equiv 1 \mod 3$.

Theorem 7.1.3. *Let $p \equiv 1 \mod 3$ be a prime.*

1. (a) *There exist integers $a,\,b \in \mathbb{Z}$ such that $a \equiv 1 \mod 3$, $b \equiv 0 \mod 3$ and $p = a^2 - ab + b^2$.*
   (b) *Let $a,\,a_1,\,b,\,b_1 \in \mathbb{Z}$ be such that $a \equiv a_1 \equiv 1 \mod 3$, $b \equiv b_1 \equiv 0 \mod 3$ and $p = a^2 - ab + b^2 = a_1^2 - a_1b_1 + b_1^2$. Then it follows that either $(a_1,b_1) = (a,b)$ or $(a_1,b_1) = (a-b,-b)$.*
2. *There exist integers $A,\,B \in \mathbb{Z}$, uniquely determined by p up to sign, such that $p = A^2 + 3B^2$.*
3. *There exist integers $L,\,M \in \mathbb{Z}$, uniquely determined by p up to sign, such that $4p = L^2 + 27M^2$.*

Proof. 1. By Lemma 7.1.1.4, $p = \mathcal{N}(\pi)$ for some prime element $\pi \equiv 1 \mod 3$ of E. If $\pi = a + b\rho$, where $a,\,b \in \mathbb{Z}$, $a \equiv 1 \bmod 3$ and $b \equiv 0 \bmod 3$, then we obtain $p = a^2 - ab + b^2$. Thus assume that we also have integers $a_1 \equiv 1 \bmod 3$ and $b_1 \equiv 0 \bmod 3$ such that $p = a_1^2 - a_1b_1 + b_1^2 = \pi_1\overline{\pi}_1$, where $\pi_1 = a_1 + b_1\rho$. Since $\pi_1 \equiv 1 \bmod 3$, we obtain (again by Lemma 7.1.1) that either $\pi_1 = \pi$ or $\pi_1 = \overline{\pi} = a + b\rho^2 = a - b - b\rho$. In the first case, we get $(a_1,b_1) = (a,b)$, and in the second case we get $(a_1,b_1) = (a-b,-b)$.

2. By 1., there exist $a,\,b \in \mathbb{Z}$ such that $p = a^2 - ab + b^2$.

CASE 1: $ab \equiv 0 \mod 2$. We may assume that $a \equiv 0 \mod 2$, and then we obtain

$$p = \Big(b - \frac{a}{2}\Big)^2 + 3\Big(\frac{a}{2}\Big)^2\,.$$

CASE 2: $a \equiv b \equiv 1 \bmod 2$. Then $p = a^2 - ab + b^2 = (b-a)^2 - b(b-a) + b^2$, and since $b - a \equiv 0 \bmod 2$, the assertion follows by CASE 1.

The unqueness of A and B follows by Theorem 3.4.2.

3. By 1., there exist $a,\, b \in \mathbb{Z}$ such that $p = a^2 - ab + b^2$ and $b \equiv 0 \bmod 3$. Then $4p = (2a-b)^2 + 3b^2 = L^2 + 27M^2$, where $L = 2a - b$ and $M = b/3$. To prove uniqueness, suppose that $L_1,\, M_1 \in \mathbb{Z}$ are any integers satisfying $4p = L_1^2 + 27M_1^2$. Then $L_1 + 3M_1 \equiv 0 \bmod 2$, and we set $L_1 + 3M_1 = 2a_1$ and $3M_1 = b_1$. We obtain $4p = (2a_1 - b_1)^2 + 3b_1^2 = 4(a_1^2 - a_1b_1 + b_1^2)$, hence $p = a_1^2 - a_1b_1 + b_1^2$, and therefore either $(a_1, b_1) = (a, b)$ or $(a_1, b_1) = (a - b, -b)$ by 1. In the first case, it follows that $M_1 = b_1/3 = b/3 = M$ and $L_1 = 2a_1 - b_1 = 2a - b = L$. In the second case, we get $M_1 = b_1/3 = -b/3 = -M$ and $L_1 = 2a_1 - b_1 = 2(a-b) + b = 2a - b = L$. $\square$

Exercise 7.1.4. Let $p \equiv 1 \bmod 3$ be a prime and $4p = L^2 + 27M^2$, where $L,\, M \in \mathbb{Z}$ and $L \equiv M \bmod 4$. Prove that $p = a^2 + 3b^2$, where

$$(a, b) = \Bigl(\frac{L}{2}, \frac{3M}{2}\Bigr) \quad \text{if} \quad L \equiv M \equiv 0 \bmod 2\,,$$

and

$$(a, b) = \Bigl(\frac{9M - L}{4}, \frac{L + 3M}{4}\Bigr) \quad \text{if} \quad L \equiv M \equiv 1 \bmod 2\,.$$

After these preparations, we define the cubic residue symbol in E which is the basic notion for our theory of cubic residues.

Theorem and Definition 7.1.5. *Let $\pi \in E \setminus \sqrt{-3}\,E$ be a prime element. Then there exists a unique character $\theta_\pi \colon (E/\pi E)^\times \to \mathbb{C}^\times$ of order 3 such that*

$$\theta_\pi(\xi) + \pi E = \xi^{(\mathsf{N}(\pi)-1)/3} \quad \textit{for all} \quad \xi \in (E/\pi E)^\times\,.$$

θ_π is called the (*normalized*) *cubic character* modulo π. If $\alpha \in E \setminus \pi E$, then $\alpha + \pi E \in (E/\pi E)^\times$, we set $\theta_\pi(\alpha) = \theta_\pi(\alpha + \pi E)$, and we define the *cubic residue symbol modulo* π by

$$\Bigl(\frac{\alpha}{\pi}\Bigr)_3 = \theta_\pi(\alpha) \in \langle \rho \rangle\,.$$

By the very definition, it follows that

$$\Bigl(\frac{\alpha}{\pi}\Bigr)_3 \equiv \alpha^{(\mathcal{N}(\pi)-1)/3} \bmod \pi \quad \text{for all} \quad \alpha \in D \setminus \pi D\,,$$

and the symbol

$$\Bigl(\frac{\alpha}{\pi}\Bigr)_3$$

depends only on the prime ideal πE and the residue class $\alpha + \pi E$ and not on π and α itself. Moreover, if $\alpha_1,\, \alpha_2 \in E \setminus \pi E$, then $\alpha_1\alpha_2 \in E \setminus \pi E$, and

$$\Bigl(\frac{\alpha_1\alpha_2}{\pi}\Bigr)_3 = \Bigl(\frac{\alpha_1}{\pi}\Bigr)_3 \Bigl(\frac{\alpha_2}{\pi}\Bigr)_3\,.$$

PROOF. We must prove existence and uniqueness of θ_π.

Suppose that $(E/\pi E)^\times = \langle\omega\rangle$. Then $\operatorname{ord}(\omega^{\mathcal{N}(\pi)-1)/3}) = 3$, and therefore $\omega^{\mathcal{N}(\pi)-1)/3} = (\rho+\pi D)^{\pm 1}$. Replacing ω by ω^{-1} if necessary, we may assume that $\omega^{\mathcal{N}(\pi)-1)/3} = \rho+\pi E$. Let $\theta_\pi\colon (E/\pi E)^\times \to \mathbb{C}^\times$ be the unique character satisfying $\theta_\pi(\omega) = \rho$ (see Corollary A.7.5.1). Then $\operatorname{ord}(\theta_\pi) = 3$, and the characters θ_π and $\theta_\pi^2 = \theta_\pi^{-1} = \overline{\theta_\pi}$ are the only characters of order 3 of $(E/\pi E)^\times$. Hence it suffices to prove that $\theta_\pi(\xi)+\pi E = \xi^{(\mathcal{N}(\pi)-1)/3}$ for all $\xi \in (E/\pi E)^\times$ (then θ_π^{-1} does not have this property).

Suppose that $\xi \in (E/\pi E)^\times$, say $\xi = \omega^k$ for some $k \in \mathbb{N}$. Then it follows that $\xi^{(\mathcal{N}(\pi)-1)/3} = (\omega^{(\mathcal{N}(\pi)-1)/3})^k = \rho^k+\pi E = \theta_\pi(\omega)^k+\pi E = \theta_\pi(\xi)+\pi E$. $\square$

It is now almost clear how the cubic residue symbol controls the cubic residue character of elements in E. To be precise, if $\beta \in E^\bullet$, then an element $\alpha \in E$ is called a *cubic residue* modulo β (in E) if $\alpha \equiv \xi^3 \bmod \beta$ for some $\xi \in E$ (equivalently, if $\alpha+\beta E$ is an 3rd power in $E/\beta E$).

Theorem 7.1.6. *Let $\pi \in E \setminus \sqrt{-3}\,E$ be a prime element.*

1. *If $\alpha \in E\setminus\pi E$, then α is an cubic residue modulo π in E if and only if*
$$\Big(\frac{\alpha}{\pi}\Big)_3 = 1\,.$$
In particular, if $\mathcal{N}(\pi) = p \equiv 1 \bmod 3$ is a prime, then an integer $a \in \mathbb{Z}$ is a cubic residue modulo π in E if and only if a is a cubic residue modulo p (in the classical sense of Section 3.1*).*
2. *If $p \equiv 2 \bmod 3$ is a prime and $a \in \mathbb{Z}\setminus p\mathbb{Z}$, then a is a cubic residue modulo p, and*
$$\Big(\frac{a}{p}\Big)_3 = 1\,.$$

PROOF. 1. Recall that $(E/\pi E)^\times$ is a cyclic group of order $\mathcal{N}(\pi)-1$. Hence the assertion follows by Theorem A.5.2.1, since
$$\Big(\frac{\alpha}{\pi}\Big)_3 = 1 \quad \text{if and only if} \quad \alpha^{(\mathcal{N}(\pi)-1)/3} \equiv 1 \bmod \pi\,.$$
If $a \in \mathbb{Z}$ and $\mathcal{N}(\pi) = p \equiv 1 \bmod 3$ is a prime, then $a+p\mathbb{Z} = a+\pi E \in E/\pi E = \mathbb{Z}/p\mathbb{Z}$. Therefore a is a cubic residue modulo p if and only if a is a cubic residue modulo π in E.

2. If $p \equiv 2 \bmod 3$ is a prime, then $(p-1,3) = 1$. Hence a is a cubic residue modulo p (in the classical sense and also in E, see Theorem 3.1.2). In particular, we obtain
$$\Big(\frac{a}{p}\Big)_3 = 1\,. \qquad \square$$

As in the theory of quadratic residues, it is convenient to extend the definition of the cubic residue symbol to composite denominators. In this way, we introduce the *cubic Jacobi symbol* as follows.

Suppose that $\beta = \varepsilon\pi_1\cdot\ldots\cdot\pi_r \in E\setminus\sqrt{-3}\,E$, where $r \in \mathbb{N}_0$, $\varepsilon \in E^\times$ and $\pi_1,\ldots,\pi_r \in E\setminus\sqrt{-3}\,E$ are prime elements. If $\alpha \in E^\bullet$, then $(\alpha,\beta) = 1$ if and only if $\alpha \notin \pi_i E$ for all $i \in [1,r]$ (see Theorem A.8.3.3). In this case, we define the *cubic Jacobi symbol* by

$$\Big(\frac{\alpha}{\beta}\Big)_3 = \prod_{j=1}^{r}\Big(\frac{\alpha}{\pi_j}\Big)_3 \in \langle\rho\rangle\,.$$

By definition, it follows that

$$\Big(\frac{\alpha}{\beta}\Big)_3 = 1 \ \text{ if } \beta \in E^\times\,, \quad \text{and} \quad \Big(\frac{\alpha}{\beta}\Big)_3 = \Big(\frac{\alpha}{\beta_1}\Big)_3\Big(\frac{\alpha}{\beta_2}\Big)_3 \ \text{ if } \beta = \beta_1\beta_2\,.$$

In the following Theorem 7.1.7 we gather those elementary properties of the cubic Jacobi symbol which we shall use in the sequel without further reference. Only in the subsequent Section 7.2 we shall prove the cubic reciprocity law.

Theorem 7.1.7. *Suppose that* $\beta \in E \setminus \sqrt{-3}\,E$.

1. *If* $\alpha_1,\, \alpha_2 \in E$ *and* $(\alpha_1,\beta) = (\alpha_2,\beta) = 1$, *then* $(\alpha_1\alpha_2,\beta) = 1$, *and*
$$\Big(\frac{\alpha_1\alpha_2}{\beta}\Big)_3 = \Big(\frac{\alpha_1}{\beta}\Big)_3\Big(\frac{\alpha_2}{\beta}\Big)_3\,.$$
2. *If* $\alpha_1,\, \alpha_2 \in E$, $(\alpha_1,\beta) = 1$ *and* $\alpha_1 \equiv \alpha_2 \bmod \beta$, *then* $(\alpha_2,\beta) = 1$, *and*
$$\Big(\frac{\alpha_1}{\beta}\Big)_3 = \Big(\frac{\alpha_2}{\beta}\Big)_3\,.$$
3. *If* $\alpha \in E$ *and* $(\alpha,\beta) = 1$, *then* $(\overline{\alpha},\overline{\beta}) = 1$, *and*
$$\overline{\Big(\frac{\alpha}{\beta}\Big)_3} = \Big(\frac{\alpha}{\beta}\Big)_3^{-1} = \Big(\frac{\alpha}{\beta}\Big)_3^{2} = \Big(\frac{\overline{\alpha}}{\overline{\beta}}\Big)_3\,.$$
4. *We have*
$$\Big(\frac{\rho}{\beta}\Big)_3 = \rho^{(\mathcal{N}(\beta)-1)/3} \quad \textit{and} \quad \Big(\frac{-1}{\beta}\Big)_3 = 1\,.$$

Proof. Suppose that $\beta = \varepsilon\pi_1\cdot\ldots\cdot\pi_r \in E \setminus \sqrt{-3}\,E$, where $\varepsilon \in E^\times$, $r \in \mathbb{N}_0$, and $\pi_1,\ldots,\pi_r \in E \setminus \sqrt{-3}\,E$ are prime elements.

1. Suppose that $\alpha_1,\, \alpha_2 \in E$ and $(\alpha_1,\beta) = (\alpha_2,\beta) = 1$. Then $(\alpha_1\alpha_2,\beta) = 1$,

$$\Big(\frac{\alpha_1\alpha_2}{\pi_i}\Big)_3 = \Big(\frac{\alpha_1}{\pi_i}\Big)_3\Big(\frac{\alpha_2}{\pi_i}\Big)_3 \quad \text{for all } i \in [1,r]\,,$$

and therefore

$$\Big(\frac{\alpha_1\alpha_2}{\beta}\Big)_3 = \prod_{i=1}^{r}\Big(\frac{\alpha_1\alpha_2}{\pi_i}\Big)_3 = \prod_{i=1}^{r}\Big(\frac{\alpha_1}{\pi_i}\Big)_3\prod_{i=1}^{r}\Big(\frac{\alpha_2}{\pi_i}\Big)_3 = \Big(\frac{\alpha_1}{\beta}\Big)_3\Big(\frac{\alpha_2}{\beta}\Big)_3\,.$$

2. Suppose that $\alpha_1,\, \alpha_2 \in E$, $(\alpha_1,\beta) = 1$ and $\alpha_1 \equiv \alpha_2 \bmod \beta$. Then it follows that $(\alpha_2,\beta) = 1$, and $\alpha_1 \equiv \alpha_2 \bmod \pi_i$ for all $i \in [1,r]$. Hence we obtain

$$\Big(\frac{\alpha_1}{\pi_i}\Big)_3 = \Big(\frac{\alpha_2}{\pi_i}\Big)_3 \quad \text{for all } i \in [1,r],$$

and therefore

$$\Big(\frac{\alpha_1}{\beta}\Big)_3 = \prod_{i=1}^{r}\Big(\frac{\alpha_1}{\pi_i}\Big)_3 = \prod_{i=1}^{r}\Big(\frac{\alpha_2}{\pi_i}\Big)_3 = \Big(\frac{\alpha_2}{\beta}\Big)_3\,.$$

3. Suppose that $\alpha \in E$ and $(\alpha, \beta) = 1$. Then there exist $x, y \in E$ such that $\alpha x + \beta y = 1$, hence $\overline{\alpha}\,\overline{x} + \overline{\beta}\,\overline{y} = 1$, and therefore $(\overline{\alpha}, \overline{\beta}) = 1$. Since $\overline{\beta} = \overline{\varepsilon}\,\overline{\pi}_1 \cdot \ldots \cdot \overline{\pi}_r$, $\overline{\varepsilon} \in E^\times$, and $\overline{\pi}_1, \ldots, \overline{\pi}_r$ are prime elements of E, it suffices to prove that

$$\overline{\Bigl(\frac{\alpha}{\pi_i}\Bigr)_3} = \Bigl(\frac{\alpha}{\pi_i}\Bigr)_3^{-1} = \Bigl(\frac{\alpha}{\pi_i}\Bigr)_3^{2} = \Bigl(\frac{\overline{\alpha}}{\overline{\pi}_i}\Bigr)_3 \quad \text{for all } \ i \in [1, r]\,.$$

Let $i \in [1, r]$ and $\mathsf{j} \in \langle \rho \rangle$ such that

$$\Bigl(\frac{\alpha}{\pi_i}\Bigr)_3 = \mathsf{j}\,, \quad \text{that is,} \quad \alpha^{(\mathcal{N}(\pi_i - 1)/3} \in \mathsf{j} + \pi E\,.$$

Then $\overline{\alpha}^{(\mathcal{N}(\overline{\pi}_i)-1)/3} = \overline{\alpha}^{(\mathcal{N}(\pi_i)-1)/3} = \overline{\alpha^{(\mathcal{N}(\pi_i)-1)/3}} \in \overline{\mathsf{j}} + \overline{\pi}E$, and therefore

$$\Bigl(\frac{\overline{\alpha}}{\overline{\pi}_i}\Bigr)_3 = \overline{\mathsf{j}} = \mathsf{j}^{-1} = \mathsf{j}^2\,.$$

4. By Lemma 7.1.1.1,

$$\Bigl(\frac{\rho}{\pi_i}\Bigr)_3 \equiv \rho^{(\mathcal{N}(\pi_i)-1)/3} \bmod \pi_i \quad \text{implies} \quad \Bigl(\frac{\rho}{\pi_i}\Bigr)_3 = \rho^{(\mathcal{N}(\pi_i)-1)/3} \quad \text{for all } \ i \in [1, r]\,.$$

Since $\mathcal{N}(\beta) = \mathcal{N}(\pi_1) \cdot \ldots \cdot \mathcal{N}(\pi_r)$, we obtain (using Lemma A.3.4),

$$\Bigl(\frac{\rho}{\beta}\Bigr)_3 = \prod_{i=1}^{r} \Bigl(\frac{\rho}{\pi_i}\Bigr)_3 = \rho^S, \quad \text{where} \quad S = \sum_{i=1}^{r} \frac{\mathcal{N}(\pi_i) - 1}{3} \equiv \frac{\mathcal{N}(\beta) - 1}{3} \mod 3\,,$$

and therefore

$$\Bigl(\frac{\rho}{\beta}\Bigr)_3 = \rho^{(\mathcal{N}(\beta)-1)/3}\,. \qquad \square$$

7.2. The cubic reciprocity law

We start with the calculation of Gauss sums for normalized cubic characters. If $\pi \in E$ is a prime element such that $\mathcal{N}(\pi) = p \equiv 1 \bmod 3$ is a prime, then the inclusion map $\mathbb{Z}/p\mathbb{Z} \to E/\pi E$, defined by $a + p\mathbb{Z} \mapsto a + \pi E$, is an isomorphism by means of which we identified these two residue class groups. In particular, the normalized cubic character $\theta_\pi \colon (E/\pi E)^\times \to \mathbb{C}^\times$ is a character modulo p, hence $\theta_\pi \in \mathsf{X}(p)$, and, as usual, we view θ_π also as a Dirichlet character $\theta_\pi \colon \mathbb{Z} \to \mathbb{C}$ modulo p. Explicitly,

$$\theta_\pi(t) = \begin{cases} \theta_\pi(t + \pi E) & \text{if} \quad t \in \mathbb{Z} \setminus p\mathbb{Z}\,, \\ \quad 0 & \text{if} \quad t \in p\mathbb{Z}\,. \end{cases}$$

We calculate the Gauss sum $\tau(\theta_\pi) \in \mathbb{Z}[\zeta_{3p}]$ and the Jacobi sum $\mathsf{J}(\theta_\pi, \theta_\pi) \in E$.

Theorem 7.2.1. *Let π be a prime element in E such that $\pi \equiv 1 \bmod 3$ and $\mathcal{N}(\pi) = p \equiv 1 \bmod 3$ is a prime. Then*

$$-\mathsf{J}(\theta_\pi, \theta_\pi) = \pi \quad \textit{and} \quad -\tau(\theta_\pi)^3 = \pi^2 \overline{\pi}\,.$$

PROOF. We start with a proof of the following two assertions:

A. $-\mathsf{J}(\theta_\pi, \theta_\pi) \equiv 1 \bmod 3$.

B. $\mathsf{J}(\theta_\pi, \theta_\pi) \equiv 0 \bmod \pi$.

Proof of **A.** We calculate $\tau(\theta_\pi) \in \mathbb{Z}[\zeta_{3p}]$ modulo 3:

$$\tau(\theta_\pi)^3 = \Bigl(\sum_{t\in\mathbb{F}_p^\times} \theta_\pi(t)\zeta_p^t\Bigr)^3 \equiv \sum_{t\in\mathbb{F}_p^\times} \theta_\pi(t)^3\zeta_p^{3t} \equiv \sum_{t\in\mathbb{F}_p^\times} \zeta_p^{3t} \equiv -1 + \sum_{t\in\mathbb{F}_p} \zeta_p^{3t} \equiv -1 \mod 3\,.$$

Hence we obtain $-\mathsf{J}(\theta_\pi,\theta_\pi) \equiv -p\,\mathsf{J}(\theta_\pi,\theta_\pi) \equiv -\tau(\theta_\pi)^3 \equiv 1 \mod 3$. □[**A.**]

Proof of **B.** We calculate $\mathsf{J}(\theta_\pi,\theta_\pi) + \pi E \in E/\pi E = \mathbb{F}_p$.

$$\mathsf{J}(\theta_\pi,\theta_\pi) + \pi E = \sum_{a\in\mathbb{F}_p^\times\setminus\{1\}} \theta_\pi(a)\theta_\pi(1-a) = \sum_{a\in\mathbb{F}_p} a^{(p-1)/3}(1-a)^{(p-1)/3} = \sum_{a\in\mathbb{F}_p} F(a)\,,$$

where $F \in \mathbb{F}_pX]$ is a polynomial of degree $\deg(F) = M = (2p-1)/3 < p-1$ and $F(0) = 0$. We set

$$F = \sum_{j=1}^{M} c_jX^j \quad \text{and obtain} \quad \mathsf{J}(\theta_\pi,\theta_\pi) + \pi E = \sum_{j=1}^{M} c_j \sum_{a\in\mathbb{F}_p^\times} a^j\,.$$

If $\mathbb{F}_p^\times = \langle\omega\rangle$, then we obtain, for every $j \in [1, p-2]$,

$$\sum_{a\in\mathbb{F}_p^\times} a^j = \sum_{\nu=0}^{p-2} \omega^{\nu j} = \frac{(\omega^j)^{p-1} - 1}{\omega^j - 1} = 0\,.$$

Hence it follows that $\mathsf{J}(\theta_\pi,\theta_\pi) + \pi E = 0 \in \mathbb{F}_p$ and thus $\mathsf{J}(\theta_\pi,\theta_\pi) \equiv 0 \mod \pi$. □[**B.**]

Suppose that **A** and **B** hold. Since $\tau(\theta_\pi)^3 = p\,\mathsf{J}(\theta_\pi,\theta_\pi)$ and $|\tau(\theta_\pi)|^2 = p$, it follows that $\mathcal{N}(\mathsf{J}(\theta_\pi,\theta_\pi)) = |\mathsf{J}(\theta_\pi,\theta_\pi)|^2 = p$, and therefore $\mathsf{J}(\theta_\pi,\theta_\pi) = \pi E$ or $\mathsf{J}(\theta_\pi,\theta_\pi) = \overline{\pi}E$. By **B** we get $\mathsf{J}(\theta_\pi,\theta_\pi)E = -\mathsf{J}(\theta_\pi,\theta_\pi)E = \pi E$, and since $-\mathsf{J}(\theta_\pi,\theta_\pi) \equiv \pi \equiv 1 \mod 3$, Lemma 7.1.1.2 implies that $-\mathsf{J}(\theta_\pi,\theta_\pi) = \pi$, and consequently $-\tau(\theta_\pi)^3 = -p\,\mathsf{J}(\theta_\pi,\theta_\pi) = -p\pi = -\pi^2\overline{\pi}$. □

Before we proceed with the cubic reciprocity law, we give another interesting application of cubic Jacobi sums.

Theorem 7.2.2. *Let* $p = 3m+1$ *be a prime, and suppose that* $4p = L^2 + 27M^2$, *where* L, $M \in \mathbb{Z}$ *and* $L \equiv 2 \mod 3$. *Then it follows that*

$$L \equiv (-1)^m \binom{2m}{m} \mod p\,.$$

Proof. We consider the prime element

$$\pi = \frac{L + 3M\sqrt{-3}}{2} \in E \quad \text{satisfying} \quad \mathcal{N}(\pi) = p \quad \text{and} \quad \pi \equiv 1 \mod 3\,.$$

We calculate $\mathsf{J}(\theta_\pi^2,\theta_\pi^2) + \pi E \in E/\pi E = \mathbb{F}_p$.

$$\begin{aligned}\mathsf{J}(\theta_\pi^2,\theta_\pi^2) + \pi E &= \sum_{a\in\mathbb{F}_p^\times\setminus\{1\}} a^{2(p-1)/3}(1-a)^{2(p-1)/3} = \sum_{a\in\mathbb{F}_p} a^{2m} \sum_{j=0}^{2m} \binom{2m}{j}(-1)^j a^j \\ &= \sum_{j=0}^{2m} (-1)^j \binom{2m}{j} \sum_{a\in\mathbb{F}_p^\times} a^{2m+j}\,.\end{aligned}$$

Suppose that $\mathbb{F}_p^\times = \langle \omega \rangle$. For $j \in [0, 2m]$ and $\nu \in [0, p-2] = [0, 3m-1]$ we have $2m + j \in [0, 5m-1]$, and thus $2m + j \equiv 0 \bmod 3m$ if and only if $j = m$ (observe that $3m = p - 1$). Hence we obtain

$$\sum_{a \in \mathbb{F}_p^\times} a^{2m+j} = \sum_{\nu=0}^{p-2} \omega^{(2m+j)\nu} = \begin{cases} -1 + p\mathbb{Z} & \text{if} \quad j = m\,, \\ \quad 0 & \text{if} \quad j \neq m\,, \end{cases}$$

and consequently

$$\mathsf{J}(\theta_\pi^2, \theta_\pi^2) \equiv (-1)^{m+1} \binom{2m}{m} \mod \pi\,.$$

On the other hand, $\mathsf{J}(\theta_\pi^2, \theta_\pi^2) = \mathsf{J}(\overline{\theta}_\pi, \overline{\theta}_\pi) = \overline{\mathsf{J}(\theta_\pi, \theta_\pi)} = -\overline{\pi}$, and therefore

$$L = \pi + \overline{\pi} \equiv \overline{\pi} \equiv -\mathsf{J}(\theta_\pi^2, \theta_\pi^2) \equiv (-1)^m \binom{2m}{m} \mod \pi\,.$$

Since both sides of this congruence are rational integers, the congruence holds modulo p. □

In the literature there are different definitions of primary elements in E used for the formulation of the cubic reciprocity law (confer [**67**] and [**44**]). Our definition combines these possibilities.

An element $\alpha \in E$ is called *primary* if $\alpha \equiv 1$ or $2 \bmod 3$. The following lemma is a simple variant of Exercise 7.1.2.

Lemma 7.2.3. *Every primary element $\alpha \in E$ has a factorization*

$$\alpha = \varepsilon \pi_1 \cdot \ldots \cdot \pi_r\,,$$

where $\varepsilon \in \{\pm 1\}$, $r \in \mathbb{N}_0$ and $\pi_1, \ldots, \pi_r$ are primary prime elements of E.

Proof. Let $\alpha \in E$ be primary. As E is factorial, $\alpha = u\widetilde{\pi}_1 \cdot \ldots \cdot \widetilde{\pi}_r$, where $u \in E^\times$, $r \in \mathbb{N}_0$, and $\widetilde{\pi}_1, \ldots, \widetilde{\pi}_r$ are prime elements of E. By Lemma 7.1.1.3, for every $i \in [1, r]$ there exists some $\varepsilon_i \in E^\times$ such that $\pi_i = \varepsilon_i \widetilde{\pi}_i$ is primary. If $\varepsilon = u\varepsilon_1 \cdot \ldots \cdot \varepsilon_r$, then $\alpha = \varepsilon \pi_1 \cdot \ldots \cdot \pi_r$, $\varepsilon \in E^\times$ and $\varepsilon \equiv \pm 1 \bmod 3$. Thus we obtain $\varepsilon = \pm 1$. □

Theorem 7.2.4 (Cubic reciprocity law)**.**

1. *If $a, b \in \mathbb{Z}$ and $(a, 3b) = 1$, then*

$$\Big(\frac{b}{a}\Big)_3 = 1\,.$$

2. *If $\alpha, \beta \in E$ are primary and $(\alpha, \beta) = 1$, then*

$$\Big(\frac{\alpha}{\beta}\Big)_3 = \Big(\frac{\beta}{\alpha}\Big)_3\,.$$

3. *Suppose that $\alpha = a + b\rho$, where $a, b \in \mathbb{Z}$, $a \equiv 1 \bmod 3$ and $b \equiv 0 \bmod 3$. Then*

$$\Big(\frac{\rho}{\alpha}\Big)_3 = \rho^{(1-a-b)/3}\,, \quad \Big(\frac{1-\rho}{\alpha}\Big)_3 = \rho^{(a-1)/3} \quad \text{and} \quad \Big(\frac{3}{\alpha}\Big) = \rho^{b/3}\,.$$

Proof. 1. If $a = \varepsilon q_1 \cdot \ldots \cdot q_r$, where $\varepsilon \in \{\pm 1\}$, $r \in \mathbb{N}_0$, and $q_1, \ldots, q_r$ are primes different from 3, then

$$\Bigl(\frac{b}{a}\Bigr)_3 = \prod_{i=1}^{r} \Bigl(\frac{b}{q_i}\Bigr)_3 \quad \text{and thus we must prove that} \quad \Bigl(\frac{b}{q}\Bigr)_3 = 1 \quad \text{for all primes } q \nmid 3b.$$

For a prime $q \equiv 2 \bmod 3$, the assertion follows by Theorem 7.1.6.2. Thus suppose that $q \equiv 1 \bmod 3$ is a prime such that $q \nmid b$. Then $q = \lambda\overline{\lambda}$ for some prime element $\lambda \in E$, and

$$\Bigl(\frac{b}{q}\Bigr)_3 = \Bigl(\frac{b}{\lambda}\Bigr)_3 \Bigl(\frac{b}{\overline{\lambda}}\Bigr)_3 = \Bigl(\frac{b}{\lambda}\Bigr)_3 \overline{\Bigl(\frac{b}{\lambda}\Bigr)_3} = 1\,.$$

2. We proceed in a series of steps.

I. Let $\pi, \lambda \in E$ be prime elements such that π is primary, $\mathcal{N}(\pi) = p \equiv 1 \bmod 3$ and $\mathcal{N}(\lambda) = q \equiv 1 \bmod 3$ are distinct primes. Then

$$\Bigl(\frac{q}{\pi}\Bigr)_3^2 = \Bigl(\frac{\pi^2\overline{\pi}}{\lambda}\Bigr)_3 .$$

Proof of **I.** We may assume that $\pi \equiv 1 \bmod 3$ (otherwise we consider $-\pi$), and we calculate the Gauss sum $\tau(\theta_\pi) \in \mathbb{Z}[\zeta_{3p}]$ modulo q as follows.

$$\tau(\theta_\pi)^q \equiv \sum_{t \in \mathbb{F}_p^\times} \theta_\pi(t)^q \zeta_p^{tq} \;\equiv\; \sum_{t \in \mathbb{F}_p^\times} \theta_\pi(t) \zeta_p^{tq} \;\equiv\; \tau(q, \theta_\pi) \;\equiv\; \overline{\theta}_\pi(q)\, \tau(\theta_\pi) \mod q\,.$$

We multiply this congruence by $\tau(\overline{\theta}_\pi)$, observe that $\tau(\theta_\pi)\tau(\overline{\theta}_\pi) = p \neq q$, cancel p and obtain

$$\tau(\theta_\pi)^{q-1} \equiv \overline{\theta}_\pi(q) \equiv \Bigl(\frac{q}{\pi}\Bigr)_3^2 \mod q\,.$$

Since

$$\tau(\theta_\pi)^{q-1} = [\tau(\theta_\pi)^3]^{(q-1)/3} = (-\pi^2\overline{\pi})^{(q-1)/3} \equiv \Bigl(\frac{-\pi^2\overline{\pi}}{\lambda}\Bigr)_3 \mod \lambda\,,$$

it follows that

$$\Bigl(\frac{\pi^2\overline{\pi}}{\lambda}\Bigr)_3 = \Bigl(\frac{-\pi^2\overline{\pi}}{\lambda}\Bigr)_3 \equiv \Bigl(\frac{q}{\pi}\Bigr)_3^2 \mod \lambda\,,$$

and therefore equality holds. □[**I.**]

II. Let $\alpha \in E$ be primary, $a \in \mathbb{Z} \setminus 3\mathbb{Z}$ and $b \in \mathbb{Z}$. Then

$$\Bigl(\frac{\alpha}{a}\Bigr)_3 = \Bigl(\frac{a}{\alpha}\Bigr)_3 .$$

Proof of **II.** Suppose that $a = \varepsilon q_1 \cdot \ldots \cdot q_r$, where $\varepsilon \in \{\pm 1\}$, $r \in \mathbb{N}_0$ and $q_1, \ldots, q_r$ are primes different from 3. By Lemma 7.2.3, $\alpha = \eta\pi_1 \cdot \ldots \cdot \pi_s$, where $\eta \in \{\pm 1\}$ and $\pi_1, \ldots, \pi_s$ are primary prime elements of E. For $j \in [1, s]$, it follows that either $\mathcal{N}(\pi_j) = p_j \equiv 1 \bmod 3$ is a prime, or $\pi_j = \pm p_j$ for some prime $p_j \equiv 2 \bmod 3$. Since

$$\Bigl(\frac{\alpha}{a}\Bigr)_3 = \prod_{i=1}^{r}\prod_{j=1}^{s} \Bigl(\frac{\pi_j}{q_i}\Bigr)_3 \quad \text{and} \quad \Bigl(\frac{a}{\alpha}\Bigr)_3 = \prod_{i=1}^{r}\prod_{j=1}^{s} \Bigl(\frac{q_i}{\pi_j}\Bigr)_3 ,$$

it suffices to prove that

$$\Bigl(\frac{\pi_j}{q_i}\Bigr)_3 = \Bigl(\frac{q_i}{\pi_j}\Bigr)_3 \quad \text{for all } i \in [1, r] \text{ and } j \in [1, s]\,.$$

If $\pi_j = \pm p_j$ for some prime $p_j \equiv 2 \bmod 3$, this follows by 1. Therefore it suffices to prove the following assertion:

IIa. If π is a primary prime element of E such that $\mathcal{N}(\pi) = p \equiv 1 \bmod 3$ is a prime and $q \nmid 3p$ is a prime, then

$$\Big(\frac{\pi}{q}\Big)_3 = \Big(\frac{q}{\pi}\Big)_3 .$$

Proof of **IIa.** CASE 1: $q \equiv 1 \bmod 3$. Let $\lambda \in E$ be a prime element such that $q = \lambda\overline{\lambda}$ and apply **I.** It follows that

$$\Big(\frac{q}{\pi}\Big)_3 = \Big(\frac{\pi^2\overline{\pi}}{\lambda}\Big)_3^2 = \Big(\frac{\pi}{\lambda}\Big)_3^4\Big(\frac{\overline{\pi}}{\lambda}\Big)_3^2 = \Big(\frac{\pi}{\lambda}\Big)_3\overline{\Big(\frac{\overline{\pi}}{\lambda}\Big)} = \Big(\frac{\pi}{\lambda}\Big)_3\Big(\frac{\pi}{\overline{\overline{\lambda}}}\Big)_3 = \Big(\frac{\pi}{q}\Big)_3 .$$

CASE 2: $q \equiv 2 \bmod 3$. We calculate the Gauss sum $\tau(\theta_\pi) \in \mathbb{Z}[\zeta_{3p}]$ modulo q.

$$\tau(\theta_\pi)^q \equiv \sum_{t\in\mathbb{F}_p^\times} \theta_\pi(t)^q\zeta_p^{tq} \;\equiv\; \sum_{t\in\mathbb{F}_p^\times} \overline{\theta}_\pi(t)\zeta_p^{tq} \;\equiv\; \tau(q,\overline{\theta}_\pi) \;\equiv\; \theta_\pi(q)\,\tau(\overline{\theta}_\pi) \bmod q .$$

We multiply this congruence by $\tau(\theta_\pi)$, observe that $\tau(\theta_\pi)\tau(\overline{\theta}_\pi) = p = \pi\overline{\pi}$ and obtain

$$\tau(\theta_\pi)^{q+1} \equiv \Big(\frac{q}{\pi}\Big)_3\pi\overline{\pi} \bmod q .$$

Recall that $\tau(\theta_\pi)^{q+1} = [\tau(\theta_\pi)^3]^{q+1)/3} = (-\pi^2\overline{\pi})^{q+1)/3}$, and if $\pi = a + b\rho$, where $a,\, b \in \mathbb{Z}$, then $\pi^q \equiv a^q + b^q\rho^2 \equiv a + b\rho^2 \equiv \overline{\pi} \bmod q$. Hence it follows that

$$\tau(\theta_\pi)^{q+1} \equiv (-\pi^{q+2})^{(q+1)/3} \equiv \Big(\frac{q}{\pi}\Big)_3\pi^{q+1} \bmod q ,$$

and since $(\pi, q) = 1$, we get

$$\Big(\frac{q}{\pi}\Big)_3 \equiv (-1)^{(q+1)/3}\pi^{(q+2)(q+1)/3-(q+1)} \equiv \pi^{(q^2-1)/3} \equiv \Big(\frac{\pi}{q}\Big)_3 \bmod q ,$$

observing that

$$\frac{(q+2)(q+1)}{3} - (q+1) = \frac{q^2-1}{3} \quad \text{and} \quad (-1)^{(q-1)/3} \equiv 1 \bmod q .$$

Therefore equality holds. □[**II.**]

III. *Proof of the general case.* Let $\alpha,\, \beta \in E$ be primary and $(\alpha,\beta) = 1$. By Lemma 7.2.3, we obtain $\alpha = \varepsilon\pi_1\cdot\ldots\cdot\pi_r$ and $\beta = \eta\lambda_1\cdot\ldots\cdot\lambda_s$, where $\varepsilon,\, \eta \in \{\pm1\}$, $r,\, s \in \mathbb{N}_0$ and $\pi_1,\ldots,\pi_r,\, \lambda_1,\ldots,\lambda_s$ are primary prime elements of E such that $\pi_i \ne \lambda_j$ for all $i \in [1,r]$ and $j \in [1,s]$. Since

$$\Big(\frac{\alpha}{\beta}\Big)_3 = \prod_{i=1}^r\prod_{j=1}^s\Big(\frac{\pi_i}{\lambda_j}\Big)_3 \quad \text{and} \quad \Big(\frac{\beta}{\alpha}\Big)_3 = \prod_{i=1}^r\prod_{j=1}^s\Big(\frac{\lambda_j}{\pi_i}\Big)_3 ,$$

it suffices to prove that

$$\Big(\frac{\pi_i}{\lambda_j}\Big)_3 = \Big(\frac{\lambda_j}{\pi_i}\Big)_3 \quad \text{for all} \;\; i \in [1,r] \;\; \text{and} \;\; j \in [1,s] .$$

By **II.**, it suffices to prove the following assertion:

IIIa. If π, $\lambda \in E$ are distinct primary prime elements such that $\mathcal{N}(\pi)$ and $\mathcal{N}(\lambda)$ are primes, then

$$\Big(\frac{\pi}{\lambda}\Big)_3 = \Big(\frac{\lambda}{\pi}\Big)_3 .$$

Proof of **IIIa.** Let π, $\lambda \in E$ be distinct primary prime elements such that $p = \pi\overline{\pi}$ and $q = \lambda\overline{\lambda}$ are primes.

CASE 1: $\lambda \ne \overline{\pi}$. By **I.** we obtain

$$\Big(\frac{q}{\pi}\Big)_3^2 = \Big(\frac{\pi^2\overline{\pi}}{\lambda}\Big)_3 \quad \text{and} \quad \Big(\frac{p}{\lambda}\Big)_3^2 = \Big(\frac{\lambda^2\overline{\lambda}}{\pi}\Big)_3 .$$

Multiplication of these two relations implies

$$\Big(\frac{\lambda}{\pi}\Big)_3 = \Big(\frac{\lambda\overline{\lambda}}{\pi}\Big)_3^2\Big(\frac{\lambda^2\overline{\lambda}}{\pi}\Big)_3 = \Big(\frac{\pi^2\overline{\pi}}{\lambda}\Big)_3\Big(\frac{\pi\overline{\pi}}{\lambda}\Big)_3^2 = \Big(\frac{\pi}{\lambda}\Big)_3 .$$

CASE 2: $\lambda = \overline{\pi}$. Since $\pi + \overline{\pi} \in \mathbb{Z} \setminus 3\mathbb{Z}$, we may apply **II.** and obtain

$$\Big(\frac{\pi}{\overline{\pi}}\Big)_3 = \Big(\frac{\pi+\overline{\pi}}{\overline{\pi}}\Big)_3 = \Big(\frac{\overline{\pi}}{\pi+\overline{\pi}}\Big)_3 = \Big(\frac{-\pi}{\pi+\overline{\pi}}\Big)_3 = \Big(\frac{\pi}{\pi+\overline{\pi}}\Big)_3 = \Big(\frac{\pi+\overline{\pi}}{\pi}\Big)_3 = \Big(\frac{\overline{\pi}}{\pi}\Big)_3 .$$

This completes the proof of 2.

3. By Theorem 7.1.7.4,

$$\Big(\frac{\rho}{\alpha}\Big) = \rho^{(\mathcal{N}(\alpha)-1)/3} = \rho^{(a^2-ab+b^2-1)/3} = \rho^{(1-a-b)/3} ,$$

since

$$a^2 - ab + b^2 + a + b - 2 = (a-1)^2 + 2a - 1 - b(a-1) + a - 2 \equiv 3(a-1) \equiv 0 \mod 9 ,$$

and therefore $a^2 - ab + b^2 - 1 \equiv 1 - a - b \mod 9$.

Next we prove that

$$(*) \qquad \Big(\frac{3\rho}{\alpha}\Big)_3 = \rho^{(1-a)/3} .$$

We set $b = 3\varepsilon m$, where $\varepsilon \in \{\pm 1\}$, $m \in \mathbb{N}_0$, and we proceed by induction on m.

$m = 0$: Then $\alpha = a$, and

$$\Big(\frac{3\rho}{a}\Big)_3 = \Big(\frac{3}{a}\Big)_3\Big(\frac{\rho}{a}\Big)_3 = \rho^{(1-a)/3} .$$

$m \ge 0$, $m \to m+1$: Suppose the assertion holds for $\alpha_1 = a + 3\varepsilon m\rho$, and consider $\alpha = \alpha_1 + 3\varepsilon\rho$. Then we obtain

$$\begin{aligned}\Big(\frac{3\rho}{\alpha}\Big)_3 &= \Big(\frac{-3\varepsilon\rho}{\alpha_1 + 3\varepsilon\rho}\Big)_3 = \Big(\frac{\alpha_1}{\alpha_1 + 3\varepsilon\rho}\Big)_3 = \Big(\frac{\alpha_1 + 3\varepsilon\rho}{\alpha_1}\Big)_3 = \Big(\frac{3\varepsilon\rho}{\alpha_1}\Big)_3 \\ &= \Big(\frac{3\rho}{\alpha_1}\Big)_3 = \rho^{(1-a)/3} ,\end{aligned}$$

which completes the proof of $(*)$.

Now it follows that

$$\Big(\frac{1-\rho}{\alpha}\Big)_3 = \Big(\frac{1-\rho}{\alpha}\Big)_3^4 = \Big(\frac{(1-\rho)^4}{\alpha}\Big)_3 = \Big(\frac{(3\rho)^2}{\alpha}\Big)_3 = \Big(\frac{3\rho}{\alpha}\Big)_3^{-1} = \rho^{(a-1)/3}$$

and

$$\Big(\frac{3}{\alpha}\Big)_3 = \Big(\frac{\rho}{\alpha}\Big)_3^{-1} \rho^{(1-a)/3} = \rho^{(a+b-1)/3+(1-a)/3} = \rho^{b/3} . \qquad \square$$

Exercise 7.2.5. Calculate the cubic Jacobi symbols

$$\Bigl(\frac{-9+4\rho}{5+8\rho}\Bigr)_3 \quad\text{and}\quad \Bigl(\frac{5+2\rho}{7+4\rho}\Bigr)_3 .$$

Hint: Use the division algorithm in E: For any $\alpha,\ \beta \in E^\bullet$, there exist $\gamma,\ \delta \in E$ such that $\alpha = \beta\gamma + \delta$ and $\mathcal{N}(\delta) < \mathcal{N}(\beta)$.

We proceed with some criteria for small numbers to be cubic residues modulo a prime $p \equiv 1 \mod 3$. For more details we refer to [**6**, Sec. 7.1], [**1**, § 57] and [**67**, Ch. 7]. Warning: There are several misprints in this section of Lemmermeyer's otherwise beautiful book [**67**].

Theorem 7.2.6. *Let* $p \equiv 1 \bmod 3$ *be a prime and* $4p = L^2 + 27M^2$, *where* $L,\ M \in \mathbb{Z}$ *and* $L \equiv M \mod 2$.

1. 3 *is a cubic residue modulo* p *if and only if* $M \equiv 0 \mod 3$.
2. *Let* $l = 3m + \sigma \ne p$ *be a prime, where* $m \in \mathbb{N}$ *and* $\sigma \in \{\pm 1\}$. *Then* l *is a cubic residue modulo* p *if and only if*

$$\sum_{\substack{j=1\\ j\equiv 1 \bmod 2}}^{m} \binom{m}{j} (-1)^{(j-1)/2}\, 3^{(3j-1)/2}\, L^{m-j} M^j \equiv 0 \mod l\,.$$

In particular:

- 2 *is a cubic residue modulo* p *if and only if* $L \equiv M \equiv 0 \mod 2$.
- *If* $l = 5$ *or* $l = 7$, *then* l *is a cubic residue modulo* p *if and only if* $LM \equiv 0 \mod l$.
- *If* $l = 11$ *or* $l = 13$, *then* l *is a cubic residue modulo* p *if and only if* $LM(L^2 - 27M^2) \equiv 0 \mod l$.

PROOF. We set $p = \pi\overline{\pi}$, where

$$\pi = \frac{L + 3M\sqrt{-3}}{2} = \frac{3M + L}{2} + 3M\rho\,.$$

Then $\pi \in E$ is primary, and by Theorem 7.1.6.1, an integer $l \in \mathbb{Z} \setminus p\mathbb{Z}$ is a cubic residue modulo p if and only if l is a cubic residue modulo π in E, and this holds if and only if

$$\Bigl(\frac{l}{\pi}\Bigr)_3 = 1\,.$$

1. By Theorem 7.2.4,3,

$$\Bigl(\frac{3}{\pi}\Bigr)_3 = \rho^M = 1 \quad\text{if and only if}\quad M \equiv 0 \mod 3\,.$$

2. We have

$$\pi^m - \overline{\pi}^m \;=\; \frac{\sqrt{-3}}{2^{m-1}}\, g_m\,, \quad\text{where}\quad g_m = \sum_{\substack{j=1\\ j\equiv 1 \bmod 2}}^{m} \binom{m}{j} (-1)^{(j-1)/2}\, 3^{(j+1)/2}\, L^{m-j} M^j\,.$$

CASE 1: $l \equiv 1 \bmod 3$. Suppose that $l = \lambda\overline{\lambda}$, where $\lambda \in E$ is primary. By the cubic reciprocity law and Theorem 7.1.7.3 we obtain

$$\Big(\frac{l}{\pi}\Big)_3 = \Big(\frac{\lambda}{\pi}\Big)_3\Big(\frac{\overline{\lambda}}{\pi}\Big)_3 = \Big(\frac{\pi}{\lambda}\Big)_3\Big(\frac{\overline{\pi}}{\lambda}\Big)_3^{-1}$$

and therefore l is a cubic residue modulo p if and only if

$$\Big(\frac{\pi}{\lambda}\Big)_3 = \Big(\frac{\overline{\pi}}{\lambda}\Big)_3, \quad \text{that is,} \quad \pi^m \equiv \overline{\pi}^m \mod \lambda\,.$$

Since $(2\sqrt{-3}, \lambda) = 1$, this holds if and only if $g_m \equiv 0 \mod \lambda$, and thus if and only if $g_m \equiv 0 \mod l$.

CASE 2: $l \equiv 2 \bmod 3$. If $\pi = a + b\rho$, where $a,\, b \in \mathbb{Z}$, then it follows that $\pi^l \equiv a^l + b^l\rho^l \equiv a + b\rho^2 \equiv \overline{\pi} \bmod l$, and by the cubic reciprocity law we obtain

$$\pi^m\Big(\frac{l}{\pi}\Big)_3 = \pi^m\Big(\frac{\pi}{l}\Big)_3 \equiv \pi^{m+(l^2-1)/3} \equiv \pi^{m+m(l-1)} \equiv \pi^{lm} \equiv \overline{\pi}^m \mod l\,.$$

Therefore l is a cubic residue modulo p if and only if $\pi^m \equiv \overline{\pi}^m \bmod l$. Hence the assertion follows since $(2^{m-1}\sqrt{-3}, l) = 1$. □

Corollary 7.2.7. *Let* $p \equiv 1 \mod 3$ *be a prime and* $p = a^2 + 3b^2$, *where* $a,\, b \in \mathbb{N}$.

1. 2 *is a cubic residue modulo p if and only if* $3 \mid b$.
2. 3 *is a cubic residue modulo p if and only if* $9 \mid b$ *or* $9 \mid a \pm b$.
3. 5 *is a cubic residue modulo p if and only if one of the following conditions holds:*
   - $5 \mid a$ *and* $3 \mid b$*;*
   - $15 \mid b$*;*
   - $15 \mid a \pm b$*;*
   - $15 \mid 2a \pm b$.

PROOF. We make use of the explicit criteria given in Theorem 7.2.6. We set

$$(L, M) = \Big(2a, \frac{2b}{3}\Big) \quad \text{if} \quad b \equiv 0 \mod 3\,,$$

and

$$(L, M) = \Big(-a \pm 3b, \frac{a \pm b}{3}\Big) \quad \text{if} \quad a \pm b \equiv 0 \mod 3\,.$$

Then it follows that $4p = L^2 + 27M^2$.

1. If $3 \mid b$, then $L \equiv M \equiv 0 \bmod 2$, and thus 2 is a cubic residue modulo p. Conversely if 2 is a cubic residue modulo p, then $L \equiv M \equiv 0 \bmod 2$, and

$$p = \Big(\frac{L}{2}\Big)^2 + 27\Big(\frac{M}{2}\Big)^2 = a^2 + 3b^2\,,$$

and by the uniqueness of a^2 and b^2 (see Theorem 7.1.3.2) it follows that $3 \mid b$.

2. If $9 \mid b$ or $9 \mid a \pm b$, then $3 \mid M$, and thus 3 is a cubic residue modulo p. Conversely, suppose that 3 is a cubic residue modulo p. Then $3 \mid M$, and thus either $9 \mid b$ or $9 \mid a \pm b$.

3. Recall that 5 is a cubic residue modulo p if and only if either $5\,|\,L$ or $5\,|\,M$.

If $5\,|\,a$ and $3\,|\,b$, then $5\,|\,L$. If $15\,|\,b$ or $15\,|\,a \pm b$, then $5\,|\,M$. If $15\,|\,2a \pm b$, then $-a \pm 2b \equiv 0 \mod 5$, $a \mp b \equiv 0 \mod 3$, and $L = -a \mp 3b \equiv -1 \pm 2b \equiv 0 \mod 5$.

Conversely, if $5\,|\,M$, then obviously $15\,|\,b$ or $15\,|\,a \pm b$. Thus assume that $5\,|\,L$. Then either $3\,|\,b$ and then $5\,|\,a$, or $-a \pm 3b \equiv 0 \mod 5$. In the latter case we obtain $a \pm 2b \equiv a \mp 3b \equiv 0 \mod 5$. □

Exercise 7.2.8. Let $p \equiv 1 \mod 3$ be a prime, $p = a^2 + 3b^2$ and $4p = L^2 + 27M^2$, where a, b, L, $M \in \mathbb{Z}$. Prove the equivalence of the following assertions:

(a) 6 is a cubic residue modulo p;

(b) Either $9\,|\,b$ or $9\,|\,2a \pm b$.

(c) Either $6\,|\,M$, or $(M, 6) = 1$ and $12\,|\,L \pm M$.

Exercise 7.2.9. Investigate whether $2 + 3\rho$ is a cubic residue modulo 11 in E.

7.3. The biquadratic Jacobi symbol

Throughout this and the following sections, let $D = \mathbb{Z}[\mathsf{i}]$ be the ring of Gaussian integers.

We start with an overview of elementary results concerning the arithmetic of D and its quotient field $K = \mathsf{q}(D) = \mathbb{Q}(\mathsf{i})$. Recall that K is a quadratic number field with discriminant $\Delta_K = -4$ (Theorem 1.1.9), $D = \mathcal{O}_{-4} = \mathcal{O}_K$ is its ring of integers (Definition 5.1.6), $D^\times = \langle \mathsf{i} \rangle$ (Theorem 5.2.1.1), and $\omega_{-4} = \mathsf{i}$ is the basis number of discriminant -4. Since $h_K = h_{-4} = 1$, it follows that D is a principal ideal domain (Theorem 5.8.6).

For every prime element $\pi \in D$, there is a unique prime $p \in \pi D$, we have $\pi D \cap \mathbb{Z} = p\mathbb{Z}$, $D/\pi D$ is a field, and $|D/\pi D| = \mathfrak{N}_{-4}(\pi D) = \mathcal{N}(\pi)$ (Theorem 5.8.1 and Definition 5.4.1). In particular,

$$(D/\pi D)^\times = \{\alpha + \pi D \mid \alpha \in D \setminus \pi D\}$$

is a cyclic group of order $\mathcal{N}(\pi) - 1$, and the inclusion $\mathbb{Z} \hookrightarrow D$ induces a monomorphism $\iota_\pi \colon \mathbb{F}_p \to D/\pi D$, given by $\iota_\pi(a + p\mathbb{Z}) = a + \pi D$ for all $a \in \mathbb{Z}$. Throughout, we shall identify $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ with its image under ι_π, and then $a + p\mathbb{Z} = a + \pi D \in D/\pi D$ for all $a \in \mathbb{Z}$.

Conversely, if p is a prime, then Theorem 5.8.8 implies that p behaves in D as follows:

1. If $p \equiv 3 \mod 4$, then p is a prime element of D, and $\mathcal{N}(p) = p^2$.
2. If $p \equiv 1 \mod 4$, then there exist a, $b \in \mathbb{N}$ such that the elements $\pi = a + b\mathsf{i}$ and $\overline{\pi} = a - b\mathsf{i}$ are prime elements of D,

$$\mathcal{N}(\pi) = \mathcal{N}(\overline{\pi}) = \pi\overline{\pi} = p = a^2 + b^2\,,$$

$D/\pi D = \{a + \pi D \mid a \in \mathbb{Z} \setminus \pi\mathbb{Z}\}$ and $D/\overline{\pi} D = \{\underline{a} + \overline{\pi} D \mid a \in \mathbb{Z} \setminus \pi\mathbb{Z}\}$. If α, $\beta \in D$, then $\alpha \equiv \beta \mod \pi$ if and only if $\overline{\alpha} \equiv \overline{\beta} \mod \overline{\pi}$, and $(\alpha, \pi) = 1$

if and only if $(\overline{\alpha},\overline{\pi})=1$. In particular, if $a,\,b\in\mathbb{Z}$, then $a\equiv b \mod \pi$ if and only if $a\equiv b \mod p$, and $(a,\pi)=1$ if and only $p\nmid a$.

3. $2=-\mathsf{i}(1+\mathsf{i})^2$, $1+\mathsf{i}$ is a prime element of D, and $\mathcal{N}(1+\mathsf{i})=2$. In particular, if $\alpha\in D$, then $(\alpha,2)=1$ if and only if $\alpha\notin(1+\mathsf{i})D$.

Consequently, if $\pi\in D\setminus(1+\mathsf{i})D$ is a prime element, then

- either $\mathcal{N}(\pi)=p\equiv 1 \mod 4$ is a prime, and $D/\pi D=\mathbb{F}_p$,
- or $\pi D=pD$ for some prime $p\equiv 3 \mod 4$, and $D/\pi D=D/pD$ is a field with p^2 elements.

In both cases, it follows that $|(D/\pi D)^\times|\equiv 0 \mod 4$, and as $-1\not\equiv 1 \mod \pi$, we obtain $\operatorname{ord}(\mathsf{i}+\pi D)=4$, and

$$\{\xi\in D/\pi D \mid \xi^4=1+\pi D\}=\{\mathsf{i}^k+\pi D \mid k\in[0,3]\,\}=\{\pm\,\mathsf{i}+\pi D,\pm 1+\pi D\}\,.$$

In the following elementary Lemma 7.3.1 we investigate the behavior of elements of D modulo powers of $(1+\mathsf{i})$. We shall tacitly use these results again and again in this chapter without further reference.

An element $\alpha\in D$ is called *primary* if $\alpha\equiv 1 \mod (1+\mathsf{i})^3$.

Lemma 7.3.1. *Suppose that* $a,\,b\in\mathbb{Z}$ *and* $\alpha=a+b\mathsf{i}$.

1. (a) $\alpha\in(1+\mathsf{i})D$ *if and only if* $a\equiv b \mod 2$, *and this holds if and only if* $2\,|\,\mathcal{N}(\alpha)$.
   (b) $\alpha\equiv 1 \mod 2$ *holds if and only if* $a\equiv 1 \mod 2$ *and* $b\equiv 0 \mod 2$, *and then* $\mathcal{N}(\alpha)\equiv 1+2b \mod 8$.
   (c) α *is primary if and only if* $b\equiv 0 \mod 2$ *and* $a+b\equiv 1 \mod 4$, *and then* $\mathcal{N}(\alpha)\equiv 3-2a \mod 16$.
2. *If* $\alpha\notin(1+\mathsf{i})D$, *then there exists a unique* $u\in D^\times$ *such that* $u\alpha$ *is primary. In particular, if* $\alpha\equiv 1 \mod 2$, *then* $u\in\{\pm 1\}$ *and* $a+b\equiv u \mod 4$.
3. *If* $\pi\in D$ *is a primary prime element, then either* $\mathcal{N}(\pi)=p\equiv 1 \mod 4$ *is a prime, or* $\pi=-q$ *for some prime* $q\equiv 3 \mod 4$.
4. *If* $\alpha\notin(1+\mathsf{i})D$, *then there exist uniquely determined* $u\in D^\times$, $r\in\mathbb{N}_0$ *and primary prime elements* $\pi_1,\ldots,\pi_r\in D$ *such that* $\alpha=u\pi_1\cdot\ldots\cdot\pi_r$. *Moreover, if* $\alpha\equiv 1 \mod 2$, *then* $u\in\{\pm 1\}$.

Proof. 1. (a) The assertion follows since

$$\frac{\alpha}{1+\mathsf{i}}=\frac{(a+b\mathsf{i})(1-\mathsf{i})}{2}=\frac{a+b}{2}+\frac{b-a}{2}\,\mathsf{i}\in D \quad\text{if and only if}\quad a\equiv b \mod 2\,,$$

and $\mathcal{N}(\alpha)=a^2+b^2\equiv a+b \mod 2$.

(b) $\alpha-1=(a-1)+b\mathsf{i}\in 2D$ holds if and only if $a-1\equiv b\equiv 0 \mod 2$. If this is the case, then $a^2\equiv 1 \mod 8$, $b^2\equiv 2b \mod 8$, and $\mathcal{N}(\alpha)=a^2+b^2\equiv 1+2b \mod 8$.

(c) Note that

$$\frac{\alpha-1}{(1+\mathsf{i})^3}=\frac{(a+b\mathsf{i}-1)(-1-\mathsf{i})}{4}=\frac{1-(a-b)}{4}+\frac{1-(a+b)}{4}\,\mathsf{i}\,.$$

Hence α is primary if and only if $a-b\equiv a+b\equiv 1 \bmod 4$, which is equivalent to $a+b\equiv 1 \bmod 4$ and $b\equiv 0 \bmod 2$. If this holds, then $a\equiv 1 \bmod 2$, $b=1-a+4u$ for some $u\in\mathbb{Z}$, and

$$\mathcal{N}(\alpha)=a^2+(1-a+4u)^2\equiv 2a^2+1-2a+8u(1-a)\equiv 3-2a \bmod 16\,.$$

2. If $\alpha\notin(1+\mathsf{i})D$, then $a+b\equiv 1 \bmod 2$ by 1.(a), and since $-\alpha=-a-b\mathsf{i}$, $\mathsf{i}\alpha=-b+a\mathsf{i}$ and $-\mathsf{i}\alpha=b-a\mathsf{i}$, there exists a unique $u\in D^\times=\{\pm1,\pm\mathsf{i}\}$ such that $u\alpha\equiv 1 \bmod (1+\mathsf{i})^3$ by 1.(c). If $\alpha\equiv 1 \bmod 2$, then $b\equiv 0 \bmod 2$ and therefore $u\in\{\pm1\}$ and $u\equiv a+b \bmod 4$.

3. Obvious by 2.

4. Suppose that $\alpha\in D\setminus(1+\mathsf{i})D$. Since D is factorial, α has a factorization $\alpha=\widetilde{u}\,\widetilde{\pi}_1\cdot\ldots\cdot\widetilde{\pi}_r$, where $\widetilde{u}\in D^\times$, $r\in\mathbb{N}_0$ and $\widetilde{\pi}_1,\ldots,\widetilde{\pi}_r\in D\setminus(1+\mathsf{i})D$ are prime elements of D. For $i\in[1,r]$, let $u_i\in D^\times$ be such that $\pi_i=u_i\widetilde{\pi}_i\equiv 1 \bmod (1+\mathsf{i})^3$. Then $u=\widetilde{u}\,(u_1\cdot\ldots\cdot u_r)^{-1}\in D^\times$, and $\alpha=u\pi_1\cdot\ldots\cdot\pi_r$. If $\alpha\equiv 1 \bmod 2$, then 2. implies $u\in\{\pm1\}$.

To prove uniqueness, assume that $\alpha=u\pi_1\cdot\ldots\cdot\pi_r=\widetilde{u}\,\widetilde{\pi}_1\cdot\ldots\cdot\widetilde{\pi}_s$, where $r,\ s\in\mathbb{N}_0$, $u,\ \widetilde{u}\in D^\times$ and $\pi_1,\ldots,\pi_r,\ \widetilde{\pi}_1,\ \ldots\widetilde{\pi}_s\in D\setminus(1+\mathsf{i})D$ are prime elements satisfying $\pi_i\equiv\widetilde{\pi}_j\equiv 1 \bmod (1+\mathsf{i})^3$ for all $i\in[1,r]$ and $j\in[1,s]$. In particular, it follows that $u^{-1}\alpha\equiv\widetilde{u}^{-1}\alpha\equiv 1 \bmod (1+\mathsf{i})^3$ and therefore $u=\widetilde{u}$ by 2. By unique factorization, we obtain $r=s$ and, after renumbering if necessary, there exist $u_1,\ldots,u_r\in D^\times$ such that $\widetilde{\pi}_i=u_i\pi_i$ for all $i\in[1,r]$. However, since $\pi_i\equiv\widetilde{\pi}_i \bmod (1+\mathsf{i})^3$, 2. implies that $u_i=1$ for all $i\in[1,r]$. □

Exercise 7.3.2. Suppose that $\alpha\in D$ and $2\nmid\mathcal{N}(\alpha)$. Prove that there exists some primary element $\beta\in D$ such that $\mathcal{N}(\beta)=\mathcal{N}(\alpha)$.

Exercise 7.3.3. Suppose that $\alpha\in D\setminus(1+\mathsf{i})D$, $s\in\mathbb{N}$ and $s\geq 3$. Prove that α possesses a unique representation $\alpha\equiv\mathsf{i}^\nu 5^\mu(-1+2\mathsf{i})^\tau \bmod (1+\mathsf{i})^s$, where $\nu\in[0,3]$ and

- $\mu,\ \nu\in[0,2^{s_0}-1]$ if $s=2s_0+1$,
- $\mu\in[0,2^{s_0-2}-1]$, $\nu\in[0,2^{s_0-1}-1]$ if $s=2s_0$.

Deduce that (in D) α is a quadratic residue modulo $(1+\mathsf{i})^s$ for every $s\geq 5$ if and only if $\alpha\equiv 1 \bmod (1+\mathsf{i})^5$.

After these preparations, we define the quadratic and biquadratic residue symbols in D. These symbols are the basic notions for the theory of biquadratic residues.

Theorem and Definition 7.3.4. *Let $\pi\in D\setminus(1+\mathsf{i})D$ be a prime element. Then there exists a unique character $\chi_\pi\colon(D/\pi D)^\times\to\mathbb{C}^\times$ of order 4 such that*

$$\chi_\pi(\xi)+\pi D=\xi^{(\mathsf{N}(\pi)-1)/4}\quad\textit{for all}\quad \xi\in(D/\pi D)^\times\,.$$

The character χ_π is called the (*normalized*) *biquadratic character* modulo π. If $\alpha\in D\setminus\pi D$, then $\alpha+\pi D\in(D/\pi D)^\times$, we set $\chi_\pi(\alpha)=\chi_\pi(\alpha+\pi D)$, and we define the *biquadratic residue symbol modulo* π by

$$\Big(\frac{\alpha}{\pi}\Big)_4=\chi_\pi(\alpha)\in\{\pm1,\pm\mathsf{i}\}\,.$$

By the very definition, it follows that

$$\Big(\frac{\alpha}{\pi}\Big)_4 \equiv \alpha^{(\mathcal{N}(\pi)-1)/4} \mod \pi \quad \text{for all} \quad \alpha \in D \setminus \pi D\,.$$

The character $\chi_\pi^2\colon (D/\pi D)^\times \to \{\pm 1\}$ is the unique quadratic character of the cyclic group $(D/\pi D)^\times$ (see Corollary A.7.5.2). For $\alpha \in D \setminus \pi D$, we define the *quadratic residue symbol modulo* π *(for* D*)* by

$$\Big(\frac{\alpha}{\pi}\Big)_2 = \chi_\pi^2(\alpha + \pi D) = \Big(\frac{\alpha}{\pi}\Big)_4^2 \in \{\pm 1\}\,.$$

It follows that

$$\Big(\frac{\alpha}{\pi}\Big)_2 \equiv \alpha^{(\mathcal{N}(\pi)-1)/2} \mod \pi \quad \text{for all} \quad \alpha \in D \setminus \pi D\,,$$

and the symbols

$$\Big(\frac{\alpha}{\pi}\Big)_4 \quad \text{and} \quad \Big(\frac{\alpha}{\pi}\Big)_2$$

depend only on the prime ideal πD and the residue class $\alpha + \pi D$ and not on π and α itself. Moreover, if $\alpha_1,\ \alpha_2 \in D \setminus \pi D$, then $\alpha_1\alpha_2 \in D \setminus \pi D$,

$$\Big(\frac{\alpha_1\alpha_2}{\pi}\Big)_4 = \Big(\frac{\alpha_1}{\pi}\Big)_4\Big(\frac{\alpha_2}{\pi}\Big)_4 \quad \text{and} \quad \Big(\frac{\alpha_1\alpha_2}{\pi}\Big)_2 = \Big(\frac{\alpha_1}{\pi}\Big)_2\Big(\frac{\alpha_2}{\pi}\Big)_2\,.$$

PROOF. We must prove existence and uniqueness of χ_π.

Suppose that $(D/\pi D)^\times = \langle\omega\rangle$. Then $\mathrm{ord}(\omega^{\mathcal{N}(\pi)-1)/4}) = 4$, and therefore $\omega^{\mathcal{N}(\pi)-1)/4} = \pm\mathsf{i} + \pi D = (\mathsf{i} + \pi D)^{\pm 1}$. Replacing ω by ω^{-1} if necessary, we may assume that $\omega^{\mathcal{N}(\pi)-1)/4} = \mathsf{i} + \pi D$. Let $\chi_\pi\colon (D/\pi D)^\times \to \mathbb{C}^\times$ be the unique character satisfying $\chi_\pi(\omega) = \mathsf{i}$ (see Corollary A.7.5.1). Then $\mathrm{ord}(\chi_\pi) = 4$, and the characters χ_π and $\chi_\pi^3 = \chi_\pi^{-1} = \overline{\chi_\pi}$ are the only characters of order 4 of $(D/\pi D)^\times$. Hence it suffices to prove that $\chi_\pi(\xi) + \pi D = \xi^{(\mathcal{N}(\pi)-1)/4}$ for all $\xi \in (D/\pi D)^\times$ (then χ_π^{-1} does not have this property).

Suppose that $\xi \in (D/\pi D)^\times$, say $\xi = \omega^k$ for some $k \in \mathbb{N}$. Then it follows that $\xi^{(\mathcal{N}(\pi)-1)/4} = (\omega^{(\mathcal{N}(\pi)-1)/4})^k = \mathsf{i}^k + \pi D = \chi_\pi(\omega)^k + \pi D = \chi_\pi(\xi) + \pi D$. □

It is now almost clear how the quadratic and the biquadratic residue symbols control the quadratic and the biquadratic residue character of elements in D. To be precise, if $\beta \in D^\bullet$ and $n \in \mathbb{N}$, then an element $\alpha \in D$ is called an *n-th power residue* modulo β (in D) if $\alpha \equiv \xi^n \mod \beta$ for some $\xi \in D$ (equivalently, if $\alpha + \beta D$ is an n-th power in $D/\beta D$). In particular, if $n = 2$ $[n = 4]$, then α is called a *quadratic* [*biquadratic*] *residue modulo* β (in D).

Theorem 7.3.5. *Let $\pi \in D \setminus (1 + \mathsf{i})D$ be a prime element.*

1. *If $\alpha \in D \setminus \pi D$ and $n \in \mathbb{N}$, then α is an n-th power residue modulo π in D if and only if*

$$\alpha^{(\mathcal{N}(\pi)-1)/(\mathcal{N}(\pi)-1,n)} \equiv 1 \mod \pi\,.$$

In particular, α is a biquadratic [quadratic] residue modulo π in D if and only if

$$\Big(\frac{\alpha}{\pi}\Big)_4 = 1 \qquad \Big[\ \Big(\frac{\alpha}{\pi}\Big)_2 = 1\ \Big]\,.$$

2. *Suppose that* $\mathcal{N}(\pi) = p \equiv 1 \bmod 4$ *is a prime,* $a \in \mathbb{Z}$ *and* $n \in \mathbb{N}$*. Then* a *is an* n*-th power residue modulo* π *in* D *if and only if* a *is an* n*-th power residue modulo* p *(in the classical sense of* Section 3.1*). In particular, if* $n = 2$*, then it follows that*
$$\Big(\frac{a}{\pi}\Big)_2 = \Big(\frac{a}{p}\Big) \quad (\textit{the Legendre symbol}).$$
3. *If* $p \equiv 3 \bmod 4$ *is a prime and* $a \in \mathbb{Z} \setminus p\mathbb{Z}$*, then*
$$\Big(\frac{a}{p}\Big)_4 = 1\,,$$
and a *is a biquadratic residue modulo* p *in* D*.*

PROOF. 1. Recall that $(D/\pi D)^\times$ is a cyclic group of order $\mathcal{N}(\pi) - 1$, and that an element $\alpha \in D \setminus \pi D$ is an n-th power residue modulo π in D if and only if $\alpha + \pi D$ is an n-th power in $(D/\pi D)^\times$. Hence the assertion follows by Theorem A.5.2.1.

2. If $a \in \mathbb{Z}$, then $(a + p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z}) = (a + \pi D \in D/\pi D)$. Hence a is an n-th power residue modulo p if and only if a is an n-th power residue modulo π in D.

3. If $p \equiv 3 \bmod 4$ is a prime, then p is a prime element of D, and $\mathcal{N}(p) = p^2$. If $a \in \mathbb{Z} \setminus p\mathbb{Z}$, then
$$\Big(\frac{a}{p}\Big)_4 \equiv a^{(p^2-1)/4} \equiv (a^{p-1})^{(p+1)/4} \equiv 1 \bmod p\,, \quad \text{hence} \quad \Big(\frac{a}{p}\Big)_4 = 1\,,$$
and a is a biquadratic residue modulo p in D by 1. □

Exercise 7.3.6. Let $\pi \in D$ be a prime element, $k,\, n \in \mathbb{N}$ and $(\mathcal{N}(\pi), n) = 1$. Prove that an element $\alpha \in D$ is an n-th power residue modulo π^k if and only if α is an n-th power residue modulo π. Hint: $|(D/\pi^k D)^\times| = \mathcal{N}(\pi)^{k-1}(\mathcal{N}(\pi) - 1)$.

As in the theory of quadratic residues, it is convenient to extend the definition of the biquadratic residue symbol to composite denominators. In this way, we introduce the *biquadratic Jacobi symbol* as follows.

Suppose that $\beta = \varepsilon\pi_1 \cdot \ldots \cdot \pi_r \in D \setminus (1+\mathsf{i})D$, where $r \in \mathbb{N}_0$, $\varepsilon \in D^\times$ and $\pi_1, \ldots, \pi_r \in D \setminus (1+\mathsf{i})D$ are prime elements. If $\alpha \in D^\bullet$, then $(\alpha, \beta) = 1$ if and only if $\alpha \notin \pi_i D$ for all $i \in [1, r]$ (see Theorem A.8.3.3). In this case, we define *biquadratic Jacobi symbol* by
$$\Big(\frac{\alpha}{\beta}\Big)_4 = \prod_{j=1}^{r} \Big(\frac{\alpha}{\pi_j}\Big)_4 \in \{\pm 1, \pm \mathsf{i}\}$$
and the *quadratic Jacobi symbol* for D by
$$\Big(\frac{\alpha}{\beta}\Big)_2 = \Big(\frac{\alpha}{\beta}\Big)_4^2 = \prod_{j=1}^{r} \Big(\frac{\alpha}{\pi_j}\Big)_2 \in \{\pm 1\}\,.$$
By definition, it follows that
$$\Big(\frac{\alpha}{\beta}\Big)_4 = 1 \ \text{ if } \beta \in D^\times\,, \quad \text{and} \quad \Big(\frac{\alpha}{\beta}\Big)_4 = \Big(\frac{\alpha}{\beta_1}\Big)_4 \Big(\frac{\alpha}{\beta_2}\Big)_4 \ \text{ if } \beta = \beta_1\beta_2\,.$$

In the following Theorem 7.3.7 we gather those elementary properties of the biquadratic Jacobi symbol which we will use in the sequel without further reference. After that, in the Theorems 7.3.8 and 7.3.9, we calculate some special biquadratic Jacobi symbols, and only in the subsequent section we shall prove the biquadratic reciprocity law and its supplement.

Theorem 7.3.7. *Suppose that* $\beta \in D \setminus (1+\mathsf{i})D$.

1. *If* $\alpha_1, \alpha_2 \in D$ *and* $(\alpha_1,\beta) = (\alpha_2,\beta) = 1$, *then* $(\alpha_1\alpha_2,\beta) = 1$, *and*
$$\Big(\frac{\alpha_1\alpha_2}{\beta}\Big)_4 = \Big(\frac{\alpha_1}{\beta}\Big)_4\Big(\frac{\alpha_2}{\beta}\Big)_4 .$$
2. *If* $\alpha_1, \alpha_2 \in D$, $(\alpha_1,\beta) = 1$ *and* $\alpha_1 \equiv \alpha_2 \mod \beta$, *then* $(\alpha_2,\beta) = 1$, *and*
$$\Big(\frac{\alpha_1}{\beta}\Big)_4 = \Big(\frac{\alpha_2}{\beta}\Big)_4 .$$
3. *If* $\alpha \in D$ *and* $(\alpha,\beta) = 1$, *then* $(\overline{\alpha},\overline{\beta}) = 1$, *and*
$$\overline{\Big(\frac{\alpha}{\beta}\Big)_4} = \Big(\frac{\alpha}{\beta}\Big)_4^{-1} = \Big(\frac{\alpha}{\beta}\Big)_4^{3} = \Big(\frac{\overline{\alpha}}{\overline{\beta}}\Big)_4 .$$
4. *If* $\varepsilon \in D^\times$, *then* $(\varepsilon,\beta) = 1$, *and*
$$\Big(\frac{\varepsilon}{\beta}\Big)_4 = \varepsilon^{(\mathcal{N}(\beta)-1)/4} .$$

Proof. Suppose that $\beta = \varepsilon\pi_1 \cdot \ldots \cdot \pi_r \in D \setminus (1+\mathsf{i})D$, where $\varepsilon \in D^\times$, $r \in \mathbb{N}_0$, and $\pi_1,\ldots,\pi_r \in D \setminus (1+\mathsf{i})D$ are prime elements.

1. If $\alpha_1, \alpha_2 \in D$ and $(\alpha_1,\beta) = (\alpha_2,\beta) = 1$, then $(\alpha_1\alpha_2,\beta) = 1$,
$$\Big(\frac{\alpha_1\alpha_2}{\pi_i}\Big)_4 = \Big(\frac{\alpha_1}{\pi_i}\Big)_4\Big(\frac{\alpha_2}{\pi_i}\Big)_4 \quad \text{for all } i \in [1,r]\,,$$
and therefore
$$\Big(\frac{\alpha_1\alpha_2}{\beta}\Big)_4 = \prod_{i=1}^r\Big(\frac{\alpha_1\alpha_2}{\pi_i}\Big)_4 = \prod_{i=1}^r\Big(\frac{\alpha_1}{\pi_i}\Big)_4\prod_{i=1}^r\Big(\frac{\alpha_2}{\pi_i}\Big)_4 = \Big(\frac{\alpha_1}{\beta}\Big)_4\Big(\frac{\alpha_2}{\beta}\Big)_4 .$$

2. Let $\alpha_1, \alpha_2 \in D$ be such that $(\alpha_1,\beta) = 1$ and $\alpha_1 \equiv \alpha_2 \mod \beta$. Then it follows that $(\alpha_2,\beta) = 1$, and $\alpha_1 \equiv \alpha_2 \mod \pi_i$ for all $i \in [1,r]$. Hence we obtain
$$\Big(\frac{\alpha_1}{\pi_i}\Big)_4 = \Big(\frac{\alpha_2}{\pi_i}\Big)_4 \quad \text{for all } i \in [1,r],$$
and therefore
$$\Big(\frac{\alpha_1}{\beta}\Big)_4 = \prod_{i=1}^r\Big(\frac{\alpha_1}{\pi_i}\Big)_4 = \prod_{i=1}^r\Big(\frac{\alpha_2}{\pi_i}\Big)_4 = \Big(\frac{\alpha_2}{\beta}\Big)_4 .$$

3. Suppose that $\alpha \in D$ and $(\alpha,\beta) = 1$. Then there exist $x, y \in D$ such that $\alpha x + \beta y = 1$, hence $\overline{\alpha}\,\overline{x} + \overline{\beta}\,\overline{y} = 1$, and therefore $(\overline{\alpha},\overline{\beta}) = 1$. Since $\overline{\beta} = \overline{\varepsilon}\,\overline{\pi}_1 \cdot \ldots \cdot \overline{\pi}_r$, $\overline{\varepsilon} \in D^\times$, and $\overline{\pi}_1,\ldots,\overline{\pi}_r$ are prime elements, it suffices to prove that
$$\overline{\Big(\frac{\alpha}{\pi_i}\Big)_4} = \Big(\frac{\alpha}{\pi_i}\Big)_4^{-1} = \Big(\frac{\alpha}{\pi_i}\Big)_4^{3} = \Big(\frac{\overline{\alpha}}{\overline{\pi}_i}\Big)_4 \quad \text{for all } i \in [1,r]\,.$$

Let $i \in [1,r]$ and $\mathsf{j} \in \{\pm\mathsf{i}, \pm 1\}$ be such that

$$\Big(\frac{\alpha}{\pi_i}\Big)_4 = \mathsf{j}\,, \quad \text{that is,} \quad \alpha^{(\mathcal{N}(\pi_i-1)/4} \in \mathsf{j} + \pi D\,.$$

Then $\overline{\alpha}^{(\mathcal{N}(\overline{\pi}_i)-1)/4} = \overline{\alpha}^{(\mathcal{N}(\pi_i)-1)/4} = \overline{\alpha^{(\mathcal{N}(\pi_i)-1)/4}} \in \overline{\mathsf{j}} + \overline{\pi}D$, and therefore

$$\Big(\frac{\overline{\alpha}}{\overline{\pi}_i}\Big)_4 = \overline{\mathsf{j}} = \mathsf{j}^{-1} = \mathsf{j}^3\,.$$

4. If $\varepsilon \in D^\times$, then $\varepsilon = \mathsf{i}^k$ for some $k \in [0,3]$. Hence

$$\Big(\frac{\varepsilon}{\pi_i}\Big)_4 \equiv \varepsilon^{(\mathcal{N}(\pi_i)-1)/4} \mod \pi_i \quad \text{implies} \quad \Big(\frac{\varepsilon}{\pi_i}\Big)_4 = \varepsilon^{(\mathcal{N}(\pi_i)-1)/4} \quad \text{for all} \quad i \in [1,r]\,.$$

Since $\mathcal{N}(\beta) = \mathcal{N}(\pi_1) \cdot \ldots \cdot \mathcal{N}(\pi_r)$, we obtain

$$\Big(\frac{\varepsilon}{\beta}\Big)_4 = \prod_{i=1}^r \Big(\frac{\varepsilon}{\pi_i}\Big)_4 = \varepsilon^S, \quad \text{where} \quad S = \sum_{i=1}^r \frac{\mathcal{N}(\pi_i)-1}{4} \equiv \frac{\mathcal{N}(\beta)-1}{4} \mod 4\,,$$

and therefore

$$\Big(\frac{\varepsilon}{\beta}\Big)_4 = \varepsilon^{(\mathcal{N}(\beta)-1)/4}\,. \qquad \square$$

Theorem 7.3.8.

1. *Suppose that* $a,\, b \in \mathbb{Z}$ *and* $\beta = a + b\mathsf{i} \in D$. *Then*

$$\Big(\frac{\mathsf{i}}{\beta}\Big)_4 = \mathsf{i}^{(1-a)/2} \quad \textit{if} \ \ \beta \ \ \textit{is primary}\,,$$

and

$$\Big(\frac{-1}{\beta}\Big)_4 = (-1)^{b/2} \quad \textit{if} \ \ \beta \equiv 1 \mod 2\,.$$

2. *If* $q \in \mathbb{Z} \setminus 2\mathbb{Z}$, *then*

$$\Big(\frac{\mathsf{i}}{q}\Big)_4 = \Big(\frac{2}{q}\Big)\,,$$

and if $q \equiv \pm 1 \bmod 8$, *then*

$$\Big(\frac{\varepsilon}{q}\Big)_4 = 1 \quad \textit{for all} \quad \varepsilon \in D^\times\,.$$

Proof. 1. If β is primary, then $\mathcal{N}(\beta) \equiv 3 - 2a \bmod 16$, and

$$\Big(\frac{\mathsf{i}}{\beta}\Big)_4 = \mathsf{i}^{(\mathcal{N}(\beta)-1)/4} = \mathsf{i}^{(1-a)/2}\,, \quad \text{since} \quad \frac{\mathcal{N}(\beta)-1}{4} \equiv \frac{1-a}{2} \mod 4\,.$$

If $\beta \equiv 1 \bmod 2$, then $\mathcal{N}(\beta) \equiv 1 + 2b \bmod 8$, and

$$\Big(\frac{-1}{\beta}\Big)_4 = (-1)^{(\mathcal{N}(\beta)-1)/4} = (-1)^{b/2}\,, \quad \text{since} \quad \frac{\mathcal{N}(\beta)-1}{4} \equiv \frac{b}{2} \mod 2\,.$$

2. If $q \in \mathbb{Z} \setminus 2\mathbb{Z}$, then $\mathcal{N}(q) = q^2$, and therefore

$$\Big(\frac{\mathsf{i}}{q}\Big)_4 = \mathsf{i}^{(q^2-1)/4} = (-1)^{(q^2-1)/8} = \Big(\frac{2}{q}\Big)\,.$$

If $q \equiv \pm 1 \bmod 8$ and $\varepsilon \in D^\times$, then $\varepsilon = \mathsf{i}^k$ for some $k \in [0,3]$, and therefore

$$\Big(\frac{\varepsilon}{q}\Big)_4 = \Big(\frac{\mathsf{i}}{q}\Big)_4^k = \Big(\frac{2}{q}\Big)^k = 1\,. \qquad \square$$

In the following Theorem 7.3.9.2, we consider congruences for fractions with a denominator coprime to the modulus, and for this we use the conventions and results of Theorem and Definition A.8.5.

Theorem 7.3.9.

1. *If* $a,\, b \in \mathbb{Z}$, $\alpha,\, \beta \in D$, $(2a,b)=1$, $(2a,\beta)=1$ *and* $(2\alpha,b)=1$, *then*

$$\Big(\frac{a}{b}\Big)_4 = 1\,, \quad \Big(\frac{\alpha}{b}\Big)_2 = \Big(\frac{\mathcal{N}(\alpha)}{b}\Big) \quad \text{and} \quad \Big(\frac{a}{\beta}\Big)_2 = \Big(\frac{a}{\mathcal{N}(\beta)}\Big)$$

(*using the ordinary rational Jacobi symbol*).

2. *Let* p *be a prime,* $\varepsilon \in \{\pm 1\}$, $p \equiv \varepsilon \bmod 4$, $a \in \mathbb{Z}\setminus p\mathbb{Z}$ *and* $p \nmid a^2+1$. *Then*

$$\frac{a+\varepsilon\mathsf{i}}{a-\varepsilon\mathsf{i}} \in D_{[p]}\,, \quad \text{and} \quad \Big(\frac{a+\mathsf{i}}{p}\Big)_4 \equiv \Big(\frac{a+\varepsilon\mathsf{i}}{a-\varepsilon\mathsf{i}}\Big)^{(p-\varepsilon)/4} \bmod p\,.$$

Proof. 1. To prove the first two assertions, we set $b = \varepsilon p_1 \cdot \ldots \cdot p_r$, where $r \in \mathbb{N}_0$, $\varepsilon \in \{\pm 1\}$ and $p_1, \ldots, p_r$ are primes. Then

$$\Big(\frac{a}{b}\Big)_4 = \prod_{i=1}^r \Big(\frac{a}{p_i}\Big)_4 = 1 \quad \text{and} \quad \Big(\frac{\alpha}{b}\Big)_2 = \prod_{i=1}^r \Big(\frac{\alpha}{p_i}\Big)_2 = \prod_{i=1}^r \Big(\frac{\mathcal{N}(\alpha)}{p_i}\Big) = \Big(\frac{\mathcal{N}(\alpha)}{b}\Big)\,.$$

Hence we may assume that b is a prime.

If $b = p \equiv 1 \bmod 4$ is a prime, then $p = \pi\overline{\pi}$ for some prime element $\pi \in D$, $(\pi, a) = 1$ and $(\pi,\alpha)=1$. Hence we obtain

$$\Big(\frac{\alpha}{p}\Big)_4 = \Big(\frac{\alpha}{\pi}\Big)_4\Big(\frac{\alpha}{\overline{\pi}}\Big)_4 = \Big(\frac{\alpha}{\pi}\Big)_4\Big(\frac{\overline{\alpha}}{\pi}\Big)_4^3 = \Big(\frac{\mathcal{N}(\alpha)}{\pi}\Big)_4\Big(\frac{\overline{\alpha}}{\pi}\Big)_4^2,$$

and therefore

$$\Big(\frac{\alpha}{p}\Big)_2 = \Big(\frac{\alpha}{p}\Big)_4^2 = \Big(\frac{\mathcal{N}(\alpha)}{\pi}\Big)_4^2 = \Big(\frac{\mathcal{N}(\alpha)}{\pi}\Big)_2 = \Big(\frac{\mathcal{N}(\alpha)}{p}\Big),$$

where the last symbol is the Legendre symbol. Obviously, we have

$$\Big(\frac{a}{p}\Big)_4 = \Big(\frac{a}{\pi}\Big)_4\Big(\frac{a}{\overline{\pi}}\Big)_4 = \Big(\frac{a}{\pi}\Big)_4\overline{\Big(\frac{a}{\pi}\Big)_4} = 1\,.$$

If $b = p \equiv 3 \bmod 4$ is a prime, then p is prime element of D, and

$$\Big(\frac{a}{p}\Big)_4 = 1$$

by Theorem 7.3.5.3.

If $\alpha = a + b\mathsf{i}$, where $a,\, b \in \mathbb{Z}$, then $\alpha^p \equiv a^p + b^p\mathsf{i}^p \equiv a - b\mathsf{i} \equiv \overline{\alpha} \bmod p$,

$$\Big(\frac{\alpha}{p}\Big)_2 \equiv \alpha^{(p^2-1)/2} \equiv (\alpha^{p+1})^{(p-1)/2} \equiv \mathcal{N}(\alpha)^{(p-1)/2} \equiv \Big(\frac{\mathcal{N}(\alpha)}{p}\Big) \bmod p\,,$$

and the congruence modulo p entails equality.

To prove the third assertion, we set $\beta = \varepsilon\pi_1 \cdot \ldots \cdot \pi_r \in D$, where $\varepsilon \in D^\times$, $r \in \mathbb{N}_0$, $\pi_1, \ldots, \pi_r$ are prime elements of D, $a \in \mathbb{Z}$ and $(2a, \beta) = 1$. Then it follows that $\pi_i \notin (1+\mathsf{i})D$, $(\pi_i, a) = 1$, $(\mathcal{N}(\pi_i), a) = 1$ for all $i \in [1, r]$,

$$\Big(\frac{a}{\beta}\Big)_2 = \prod_{i=1}^r \Big(\frac{a}{\pi_i}\Big)_2 \quad\text{and}\quad \Big(\frac{a}{\mathcal{N}(\beta)}\Big) = \prod_{i=1}^r \Big(\frac{a}{\mathcal{N}(\pi_i)}\Big)\,.$$

Hence we may assume that β is a prime element of D.

If β is a prime element of D such that $\mathcal{N}(\beta) = p \equiv 1 \mod 4$ is a prime, then

$$\Big(\frac{a}{\beta}\Big)_2 = \Big(\frac{a}{p}\Big)$$

by Theorem 7.3.5.2. If $\beta = p \equiv 3 \mod 4$ is a prime, then

$$\Big(\frac{a}{p}\Big)_2 = \Big(\frac{a}{p}\Big)_4^2 = 1 \quad\text{and}\quad \Big(\frac{a}{\mathcal{N}(p)}\Big) = \Big(\frac{a}{p^2}\Big) = \Big(\frac{a}{p}\Big)^2 = 1\,.$$

2. Since $\mathcal{N}(a - \mathsf{i}\varepsilon) = a^2 + 1 \not\equiv 0 \mod p$, it follows that

$$\frac{a+\varepsilon\mathsf{i}}{a-\varepsilon\mathsf{i}} = \frac{(a+\varepsilon\mathsf{i})^2}{a^2+1} \in D_{[p]}\,,$$

and we apply Theorem A.8.5.

If $\varepsilon = 1$, then $p = \pi\overline{\pi}$ for some prime element $\pi \in D$,

$$\begin{aligned}\Big(\frac{a+\mathsf{i}}{p}\Big)_4 = \Big(\frac{a+\mathsf{i}}{\pi}\Big)_4\Big(\frac{a+\mathsf{i}}{\overline{\pi}}\Big)_4 &= \Big(\frac{a+\mathsf{i}}{\pi}\Big)_4\Big(\frac{a-\mathsf{i}}{\pi}\Big)_4^{-1} \equiv \Big(\frac{a+\mathsf{i}}{a-\mathsf{i}}\Big)^{(p-1)/4} \mod \pi\\ &= \Big(\frac{a-\mathsf{i}}{\overline{\pi}}\Big)_4^{-1}\Big(\frac{a+\mathsf{i}}{\overline{\pi}}\Big)_4 \equiv \Big(\frac{a+\mathsf{i}}{a-\mathsf{i}}\Big)^{(p-1)/4} \mod \overline{\pi}\,,\end{aligned}$$

and therefore the congruence holds modulo p.

If $\varepsilon = -1$, then p is a prime element of D, $(a+\mathsf{i})^p \equiv a^p + \mathsf{i}^p \equiv a - \mathsf{i} \mod p$, and

$$\Big(\frac{a+\mathsf{i}}{p}\Big)_4 \equiv (a+\mathsf{i})^{(p^2-1)/4} \equiv \big[(a+\mathsf{i})^{p-1}\big]^{(p+1)/4} \equiv \Big(\frac{a-\mathsf{i}}{a+\mathsf{i}}\Big)^{(p+1)/4} \mod p\,. \qquad \square$$

7.4. The biquadratic reciprocity law

We start with the calculation of the Gauss sum for a normalized biquadratic character. If $\pi \in D$ is a prime element such that $\mathcal{N}(\pi) = p \equiv 1 \mod 4$ is a prime, then the inclusion map $\mathbb{Z}/p\mathbb{Z} \to D/\pi D$, defined by $a + p\mathbb{Z} \mapsto a + \pi D$, is an isomorphism by means of which we identified these two residue class groups. In particular, the normalized biquadratic character $\chi_\pi \colon (D/\pi D)^\times \to \mathbb{C}^\times$ is a character modulo p, hence $\chi_\pi \in \mathsf{X}(p)$, and, as usual, we view χ_π also as a Dirichlet character $\chi_\pi \colon \mathbb{Z} \to \mathbb{C}$ modulo p. Explicitly,

$$\chi_\pi(t) = \begin{cases} \chi_\pi(t + \pi D) & \text{if} \quad t \in \mathbb{Z} \setminus p\mathbb{Z}\,,\\ \quad 0 & \text{if} \quad t \in p\mathbb{Z}\,. \end{cases}$$

We calculate the Gauss sum $\tau(\chi_\pi) \in \mathbb{Z}[\zeta_{4p}]$ and the Jacobi sum $\mathsf{J}(\chi_\pi, \chi_\pi) \in D$.

Theorem 7.4.1. *Let* $\pi \in D$ *be a primary prime element, and suppose that* $\mathcal{N}(\pi) = p \equiv 1 \bmod 4$. *Then*

$$-\chi_\pi(-1)\mathsf{J}(\chi_\pi, \chi_\pi) = \pi \quad \textit{and} \quad \tau(\chi_\pi)^4 = \pi^3\overline{\pi}\,.$$

Proof. We start with a proof of the following two assertions:

A. $-\chi_\pi(-1)\,\mathsf{J}(\chi_\pi, \chi_\pi) \equiv 1 \bmod (1+\mathsf{i})^3$.

B. $\mathsf{J}(\chi_\pi, \chi_\pi) \equiv 0 \bmod \pi$.

Proof of **A.** We calculate

$$\begin{aligned}
\mathsf{J}(\chi_\pi, \chi_\pi) &= \sum_{a \in \mathbb{F}_p^\times \setminus \{1\}} \chi_\pi(a)\chi_\pi(1-a) = \Big\{ \sum_{t=2}^{(p-1)/2} + \sum_{t=(p+1)/2}^{p-1} \Big\} \chi_\pi(t)\chi_\pi(1-t) \\
&=_{[1-t=u]} \sum_{t=2}^{(p-1)/2} \chi_\pi(t)\chi_\pi(1-t) + \sum_{u=2}^{(p+1)/2} \chi_\pi(u)\chi_\pi(1-u) \\
&= 2\sum_{t=2}^{(p-1)/2} \chi_\pi(t)\chi_\pi(1-t) + \chi_\pi\Big(\frac{p+1}{2}\Big)\chi_\pi\Big(1-\frac{p+1}{2}\Big),
\end{aligned}$$

and

$$\chi_\pi\Big(\frac{p+1}{2}\Big)\chi_\pi\Big(1-\frac{p+1}{2}\Big) = \chi_\pi\Big(\frac{1-p^2}{4}\Big) = \chi_\pi\Big(\frac{p^2-1}{(1+\mathsf{i})^4}\Big) = \chi_\pi(p^2-1) = \chi_\pi(-1)\,.$$

If $t \in [2, (p-1)/2\,]$, then $\chi_\pi(t)\chi_\pi(1-t) \in D^\times$, hence

$$\chi_\pi(t)\chi_\pi(1-t) \equiv 1 \bmod (1+\mathsf{i}) \quad \text{and} \quad 2\chi_\pi(t)\chi_\pi(1-t) \equiv 2 \mod (1+\mathsf{i})^3\,.$$

Since $p-3 \equiv 2 \bmod (1+\mathsf{i})^3$, $2\chi_\pi(-1) \equiv 2 \bmod (1+\mathsf{i})^3$ and $\chi_\pi(-1)^2 = \chi_\pi^2(-1) = 1$, we obtain

$$-\chi_\pi(-1)\mathsf{J}(\chi_\pi, \chi_\pi) \equiv -\chi_\pi(-1)[p-3+\chi_\pi(-1)] \equiv 2\chi_\pi(-1) - 1 \equiv 1 \bmod (1+\mathsf{i})^3\,,$$

which competes the proof of **A.**

Proof of **B.** We calculate $\mathsf{J}(\chi_\pi, \chi_\pi) + \pi D \in \mathbb{F}_p$. For $a \in \mathbb{F}_p^\times$ we have

$$\chi_\pi(a) + \pi D = a^{(\mathcal{N}(\pi)-1)/4} = a^P\,, \quad \text{where} \quad P = \frac{p-1}{4}\,,$$

and we suppose that $\mathbb{F}_p^\times = \langle\omega\rangle = \{\omega^\nu \mid \nu \in [0, p-2\,]\,\}$. Then we obtain

$$\begin{aligned}
\mathsf{J}(\chi_\pi, \chi_\pi) + \pi D &= \sum_{a \in \mathbb{F}_p^\times \setminus \{1\}} a^P(1-a)^P = \sum_{a \in \mathbb{F}_p^\times} a^P \sum_{j=0}^{P} \binom{P}{j}(-1)^j a^j \\
&= \sum_{j=0}^{P} \binom{P}{j}(-1)^j \sum_{a \in \mathbb{F}_p^\times} a^{P+j} = \sum_{j=0}^{P} \binom{P}{j}(-1)^j \sum_{\nu=0}^{p-2} \omega^{\nu(P+j)} \\
&= \sum_{j=0}^{P} \binom{P}{j}(-1)^j \frac{\omega^{(P+j)(p-1)} - 1}{\omega^{P+j} - 1} = 0 \in \mathbb{F}_p\,,
\end{aligned}$$

which completes the proof of **B.**

Suppose that **A** and **B** hold. Since χ_π^2 is the quadratic character modulo p, it follows that $\chi_\pi^2 \ne \mathbf{1}$, $\chi_\pi^2(-1) = (-1)^{(p-1)/2} = 1$, $|\mathsf{J}(\chi_\pi,\chi_\pi)|^2 = p = \pi\overline{\pi}$, and **B** implies $-\chi_\pi(-1)\mathsf{J}(\chi_\pi,\chi_\pi)D = \mathsf{J}(\chi_\pi,\chi_\pi)D = \pi D$. Hence there exists some $\varepsilon \in D^\times$ such that $-\chi_\pi(-1)\mathsf{J}(\chi_\pi,\chi_\pi) = \varepsilon\pi$. Since $-\chi_\pi(-1)\mathsf{J}(\chi_\pi,\chi_\pi) \equiv 1 \equiv \pi \bmod (1+\mathrm{i})^3$, it follows that

$$-\chi_\pi(-1)\mathsf{J}(\chi_\pi,\chi_\pi) = \pi\,,$$

and consequently

$$\mathsf{J}(\chi_\pi,\chi_\pi)^2 = [-\chi_\pi(-1)^{-1}\pi]^2 = \chi_\pi^2(-1)\pi^2\,.$$

Since $\tau(\chi_\pi)^2 = \tau(\chi_\pi^2)\mathsf{J}(\chi_\pi,\chi_\pi)$ and $\tau(\chi_\pi^2)^2 = \tau(\chi_\pi^2)\tau(\overline{\chi_\pi^2}) = \chi_\pi^2(-1)p = \chi_\pi^2(-1)\pi\overline{\pi}$, it follows that

$$\tau(\chi_\pi)^4 = \tau(\chi_\pi^2)^2\mathsf{J}(\chi_\pi,\chi_\pi)^2 = [\,\chi_\pi^2(-1)\pi\overline{\pi}\,]\,[\,\chi_\pi^2(-1)\pi^2\,] = \pi^3\overline{\pi}\,. \qquad \square$$

Exercise 7.4.2. Let $p = 4m+1 = a^2+b^2$ be a prime, where $a,\,b \in \mathbb{Z}$ and $a+b\mathrm{i} \equiv 1 \bmod (1+\mathrm{i})^3$. Prove Gauss' congruence

$$2a \equiv (-1)^m\binom{2m}{m} \mod p\,.$$

Hint: Calculate $\mathsf{J}(\chi_\pi^2,\chi_\pi^3)$ and proceed as in Theorem 7.2.2.

Now we apply Theorem 7.4.1 to obtain a weak version of a biquadratic reciprocity law.

Theorem 7.4.3 (Weak biquadratic reciprocity law)**.** *If* $q \in \mathbb{Z}\setminus 2\mathbb{Z}$, $\alpha \in D$, $(\alpha,q) = 1$ *and* $\alpha \equiv 1 \bmod 2$, *then*

$$\Big(\frac{\alpha}{q}\Big)_4 = \Big(\frac{q^*}{\alpha}\Big)_4, \quad \textit{where} \quad q^* = (-1)^{(q-1)/2}q\,.$$

Proof. CASE A: $\alpha = \pi$ be a prime element such that $\pi \equiv 1 \bmod (1+\mathrm{i})^3$ and $\mathcal{N}(\pi) = p \equiv 1 \bmod 4$ is a prime.

CASE A.1: q is a prime. We calculate the Gauss sum $\tau(\chi_\pi) \in \mathbb{Z}[\zeta_{4p}]$ modulo q and obtain

$$\tau(\chi_\pi)^q \equiv \sum_{t\in\mathbb{F}_p^\times}\chi_\pi(t)^q\zeta_p^{tq} \equiv \sum_{t\in\mathbb{F}_p^\times}\chi_\pi^q(t)\zeta_p^{tq} \equiv \tau(q,\chi_\pi^q) \equiv \overline{\chi}_\pi^q(q)\,\tau(\chi_\pi^q) \mod q\,.$$

CASE A.1a: $q \equiv 3 \bmod 4$. Then q is a prime element of D, $q^* = -q$,

$$\chi_\pi^q = \chi_\pi^3 = \overline{\chi}_\pi \quad\text{and}\quad \overline{\chi}_\pi^q = \chi_\pi\,.$$

If $a,\,b \in \mathbb{Z}$ and $\pi = a+b\mathrm{i}$, then $\pi^q \equiv a^q + b^q\mathrm{i}^q \equiv a - b\mathrm{i} \equiv \overline{\pi} \bmod q$, and therefore $\pi^{q+1} \equiv \pi\overline{\pi} \equiv p \bmod q$. Hence we obtain

$$\begin{aligned}\tau(\chi_\pi)^{q+1} &\equiv \overline{\chi}_\pi^q(q)\,\tau(\chi_\pi^q)\tau(\chi_\pi) \equiv \chi_\pi(q)\,\tau(\overline{\chi}_\pi)\tau(\chi_\pi) \equiv \chi_\pi(q)\chi_\pi(-1)\pi\overline{\pi}\\ &\equiv \Big(\frac{-q}{\pi}\Big)_4\pi^{q+1} \mod q\,,\end{aligned}$$

and

$$\tau(\chi_\pi)^{q+1} = [\tau(\chi_\pi)^4]^{(q+1)/4} = (\pi^3\overline{\pi})^{(q+1)/4} \equiv \pi^{(3+q)(q+1)/4} \mod q\,.$$

Consequently,

$$\Big(\frac{-q}{\pi}\Big)_4\pi^{q+1} \equiv \pi^{(3+q)(q+1)/4} \mod q\,,$$

and since $(\pi,q)=1$, we may cancel π^{q+1} in this congruence. It follows that

$$\Big(\frac{-q}{\pi}\Big)_4 \equiv \pi^{(q+1)[(3+q)/4-1]} \equiv \pi^{(q^2-1)/4} \equiv \Big(\frac{\pi}{q}\Big)_4 \mod q\,,$$

and therefore equality holds.

CASE A.1b: $q \equiv 1 \mod 4$. Then $q^* = q = \lambda\overline{\lambda} = \mathcal{N}(\lambda)$ for some prime element $\lambda \in D$, $\chi_\pi^q = \chi_\pi$, and

$$\begin{aligned}\tau(\chi_\pi)^{q-1}p &= \tau(\chi_\pi)^{q-1}\tau(\chi_\pi)\tau(\overline{\chi}_\pi)\chi_\pi(-1) = \tau(\chi_\pi)^{q}\tau(\overline{\chi}_\pi)\chi_\pi(-1)\\ &\equiv \overline{\chi}_\pi^{q}(q)\tau(\chi_\pi^{q})\tau(\overline{\chi}_\pi)\chi_\pi(-1) \equiv \overline{\chi}_\pi(q)\tau(\chi_\pi)\tau(\overline{\chi}_\pi)\chi_\pi(-1)\\ &\equiv \overline{\chi}_\pi(q)p \equiv \Big(\frac{q}{\pi}\Big)_4^{-1} p \mod q\,.\end{aligned}$$

Since $(p,q)=1$, we may cancel p in this congruence, and we obtain

$$\Big(\frac{\pi^3\overline{\pi}}{\lambda}\Big)_4 \equiv (\pi^3\overline{\pi})^{(\mathcal{N}(\lambda)-1)/4} \equiv \big[\tau(\chi_\pi)^4\big]^{(q-1)/4} \equiv \tau(\chi_\pi)^{q-1} \equiv \Big(\frac{q}{\pi}\Big)_4^{-1} \mod q\,.$$

Hence equality holds, and therefore

$$\Big(\frac{q}{\pi}\Big)_4 = \Big(\frac{\pi^3\overline{\pi}}{\lambda}\Big)_4^{-1} = \Big[\Big(\frac{\pi}{\lambda}\Big)_4^3\Big(\frac{\overline{\pi}}{\lambda}\Big)_4\Big]^{-1} = \Big(\frac{\pi}{\lambda}\Big)_4\Big(\frac{\pi}{\overline{\lambda}}\Big)_4 = \Big(\frac{\pi}{q}\Big)_4\,.$$

CASE A.2: $q = \varepsilon q_1 \cdot \ldots \cdot q_r \in \mathbb{Z}$, where $\varepsilon \in \{\pm 1\}$, $r \in \mathbb{N}_0$ and $q_1,\ldots,q_r$ are odd primes. Then

$$q^* = \Big(\frac{-1}{q}\Big)q \;=\; \Big[\Big(\frac{-1}{\varepsilon}\Big)\varepsilon\Big]\prod_{i=1}^{r}\Big[\Big(\frac{-1}{q_i}\Big)q_i\Big] \;=\; \prod_{i=1}^{r} q_i^*$$

and

$$\Big(\frac{q^*}{\pi}\Big)_4 \;=\; \prod_{i=1}^{r}\Big(\frac{q_i^*}{\pi}\Big)_4 \;=\; \prod_{i=1}^{r}\Big(\frac{\pi}{q_i}\Big)_4 \;=\; \Big(\frac{\pi}{q}\Big)_4\,.$$

CASE B: $\alpha \in D$, $(\alpha,q)=1$ and $\alpha \equiv 1 \mod 2$. By Lemma 7.3.1.4, there exists a (unique) factorization $\alpha = \varepsilon\pi_1 \cdot \ldots \cdot \pi_r(-q_1)\cdot\ldots(-q_s)$, where $\varepsilon \in \{\pm 1\}$, $r,\, s \in \mathbb{N}_0$, $\pi_1,\ldots\pi_r \in D$ are prime elements of D such that $\pi_i \equiv 1 \mod (1+\mathrm{i})^3$ and $\mathcal{N}(\pi_i) = p_i \equiv 1 \mod 4$ are primes for all $i \in [1,r]$, and $q_j \equiv 3 \mod 4$ are primes for all $j \in [1,s]$. Since

$$\Big(\frac{q^*}{\varepsilon}\Big)_4 = \Big(\frac{\varepsilon}{q}\Big)_4 = 1 \quad\text{and}\quad \Big(\frac{q^*}{-q_j}\Big)_4 = \Big(\frac{-q_j}{q}\Big)_4 = 1 \quad\text{for all}\quad j \in [1,s]\,,$$

it follows by CASE A that

$$\Big(\frac{q^*}{\alpha}\Big)_4 = \Big(\frac{q^*}{\varepsilon}\Big)_4\prod_{i=1}^{r}\Big(\frac{q^*}{\pi_i}\Big)_4\prod_{j=1}^{s}\Big(\frac{q^*}{-q_j}\Big)_4 = \prod_{i=1}^{r}\Big(\frac{\pi_i}{q}\Big)_4\prod_{j=1}^{s}\Big(\frac{-q_j}{q}\Big)_4 = \Big(\frac{\alpha}{q}\Big)_4\,. \qquad \square$$

Example 7.4.4. We use the weak biquadratic reciprocity law to derive criteria for the biquadratic residue character of 3 and 5. In a more systematic and more general way we shall return to criteria for biquadratic residues in the Examples 7.5.11 and 7.6.5.

Let $p \equiv 1 \bmod 4$ be a prime and $p = a^2 + b^2$, where $a,\, b \in \mathbb{Z}$ and $b \equiv 0 \bmod 2$. Then $p = \pi\overline{\pi}$, where $\pi = a + b\mathsf{i} \in D$ is a prime element and $\pi \equiv 1 \bmod 2$. If $a \in \mathbb{Z}$, then a is a biquadratic residue modulo p if and only if

$$\Big(\frac{a}{\pi}\Big)_4 = 1\,, \quad \text{and if} \quad a \equiv 1 \bmod 4\,, \quad \text{then} \quad \Big(\frac{a}{\pi}\Big)_4 = \Big(\frac{\pi}{a}\Big)_4\,.$$

$a = -3$: 3 is a prime element of D, and

$$\Big(\frac{-3}{\pi}\Big)_4 = \Big(\frac{\pi}{-3}\Big)_4 = \Big(\frac{\pi}{3}\Big)_4 \equiv \pi^2 \bmod 3\,.$$

Now it is easy to see that $\pi^2 = a^2 - b^2 + 2ab\mathsf{i} \equiv 1 \bmod 3$ if and only if $b \equiv 0 \bmod 3$. Hence -3 is a biquadratic residue modulo p if and only if $b \equiv 0 \bmod 3$.

$a = 5$: $5 = (2+\mathsf{i})(2-\mathsf{i})$, and $\mathcal{N}(2+\mathsf{i}) = \mathcal{N}(2-\mathsf{i}) = 5$. Hence we obtain

$$\Big(\frac{5}{\pi}\Big)_4 = \Big(\frac{\pi}{5}\Big)_4 = \Big(\frac{\pi}{2+\mathsf{i}}\Big)_4 \Big(\frac{\pi}{2-\mathsf{i}}\Big)_4 = 1$$

if and only if

$$\Big(\frac{\pi}{2+\mathsf{i}}\Big)_4 = \overline{\Big(\frac{\pi}{2-\mathsf{i}}\Big)_4} = \Big(\frac{\overline{\pi}}{2+\mathsf{i}}\Big)_4\,,$$

that is, if and only if $\pi \equiv \overline{\pi} \bmod 2+\mathsf{i}$. Since

$$\frac{\pi - \overline{\pi}}{2+\mathsf{i}} = \frac{2\mathsf{i}b(2-\mathsf{i})}{5} = \frac{2b+4\mathsf{i}b}{5} \in D \quad \text{if and only if} \quad b \equiv 0 \mod 5\,,$$

it follows that 5 is a biquadratic residue modulo p if and only if $b \equiv 0 \bmod 5$.

Exercise 7.4.5. Let $p = a^2 + b^2 \equiv 1 \bmod 4$ be a prime, where $a,\, b \in \mathbb{Z}$. Prove that -7 is a biquadratic residue modulo p if and only if $7 \,|\, ab$.

Before we prove the general biquadratic reciprocity law, we present a further application of the weak law.

Theorem 7.4.6. *Let* $p = a^2 + b^2 \equiv 1 \bmod 4$ *be a prime, where* $a,\, b \in \mathbb{Z}$ *and* $b \equiv 0 \bmod 2$.

1. *If* $p \equiv 1 \bmod 8$, *then* b *is a biquadratic residue modulo* p.
2. *If* $p \equiv 5 \bmod 8$ *and* $b = 2b_0$, *where* $b_0 \equiv 1 \bmod 4$, *then* b_0 *is a biquadratic residue modulo* p.

PROOF. We set $\pi = a + b\mathsf{i}$. Then π is a prime element of D, $\mathcal{N}(\pi) = p$, and an integer c is a biquadratic residue modulo p if and only if

$$\Big(\frac{c}{\pi}\Big)_4 = 1\,.$$

1. If $p \equiv 1 \bmod 8$, then $b \equiv 0 \bmod 4$, and replacing a by $-a$ if necessary, we may assume that $a \equiv 1 \bmod 4$ and thus $\pi \equiv 1 \bmod (1+\mathsf{i})^3$. Since $b \equiv \mathsf{i}a \bmod \pi$, we obtain

$$\begin{aligned}\Big(\frac{b}{\pi}\Big)_4 &= \Big(\frac{\mathsf{i}a}{\pi}\Big)_4 = \Big(\frac{\mathsf{i}}{\pi}\Big)_4\Big(\frac{a}{\pi}\Big)_4 = \Big(\frac{\mathsf{i}}{\pi}\Big)_4\Big(\frac{\pi}{a}\Big)_4 = \Big(\frac{\mathsf{i}}{\pi}\Big)_4\Big(\frac{b\mathsf{i}}{a}\Big)_4 = \Big(\frac{\mathsf{i}}{\pi}\Big)_4\Big(\frac{\mathsf{i}}{a}\Big)_4\Big(\frac{b}{a}\Big)_4 \\ &= \Big(\frac{\mathsf{i}}{\pi a}\Big)_4 = \mathsf{i}^{(1-a^2)/2} = 1\,, \quad \text{since} \quad \pi a = a^2 + abi \equiv 1 \bmod (1+\mathsf{i})^3\,.\end{aligned}$$

2. Since $\pi = a + 2b_0\mathsf{i}$, it follows that

$$\Big(\frac{b_0}{\pi}\Big)_4 = \Big(\frac{\pi}{b_0}\Big)_4 = 1\,. \qquad \square$$

Theorem 7.4.7 (Biquadratic reciprocity law)**.** *Let* $\alpha,\, \gamma \in D \setminus (1+\mathsf{i})D$ *be such that* $(\alpha,\gamma) = 1$, $\alpha = a + b\mathsf{i}$ *and* $\gamma = c + d\mathsf{i}$, *where* $a,\, b,\, c,\, d \in \mathbb{Z}$.

1. (Jacobi, Kaplan) *If* $a \equiv c \equiv 1 \bmod 4$ *and* $b \equiv d \equiv 0 \bmod 2$, *then*

$$\Big(\frac{\gamma}{\alpha}\Big)_4 = \Big(\frac{\alpha}{\gamma}\Big)_4 (-1)^{bd/4}\,.$$

2. (Gauss, Eisenstein) *If* $\alpha \equiv \gamma \equiv 1 \bmod (1+\mathsf{i})^3$, *then*

$$\Big(\frac{\gamma}{\alpha}\Big)_4 = \Big(\frac{\alpha}{\gamma}\Big)_4 (-1)^{bd/4} = \Big(\frac{\alpha}{\gamma}\Big)_4 (-1)^{\frac{a-1}{2}\,\frac{c-1}{2}} = \Big(\frac{\alpha}{\gamma}\Big)_4 (-1)^{\frac{\mathcal{N}(\alpha)-1}{4}\,\frac{\mathcal{N}(\gamma)-1}{4}}\,.$$

PROOF. 1. CASE 1: $(a,b) = (c,d) = 1$. Then it follows that

$$(a,\alpha) = (c,\gamma) = (c\alpha,\gamma) = (a\gamma,\alpha) = 1\,, \quad c\mathsf{i} \equiv d \mod \gamma \ \text{ and } \ a\mathsf{i} \equiv b \mod \alpha\,.$$

Therefore we obtain $c\alpha = ac + bc\mathsf{i} \equiv ac + bd \bmod \gamma$, $a\gamma = ac + ad\mathsf{i} \equiv ac + bd \bmod \alpha$, and consequently

$$\Big(\frac{c}{\gamma}\Big)_4\Big(\frac{\alpha}{\gamma}\Big)_4 = \Big(\frac{c\alpha}{\gamma}\Big)_4 = \Big(\frac{ac+bd}{\gamma}\Big)_4 \quad \text{and} \quad \Big(\frac{a}{\alpha}\Big)_4\Big(\frac{\gamma}{\alpha}\Big)_4 = \Big(\frac{a\gamma}{\alpha}\Big)_4 = \Big(\frac{ac+bd}{\alpha}\Big)_4,$$

which implies

$$\Big(\frac{\alpha}{\gamma}\Big)_4 = \Big(\frac{c}{\gamma}\Big)_4^{-1}\Big(\frac{ac+bd}{\gamma}\Big)_4\Big(\frac{ac+bd}{\alpha}\Big)_4^{-1}\Big(\frac{a}{\alpha}\Big)_4\Big(\frac{\gamma}{\alpha}\Big)_4 = \Big(\frac{\gamma}{\alpha}\Big)_4\Big(\frac{a}{\alpha}\Big)_4\Big(\frac{c}{\overline{\gamma}}\Big)_4\Big(\frac{ac+bd}{\gamma\overline{\alpha}}\Big)_4.$$

Since $a \equiv c \equiv ac + bd \equiv 1 \bmod 4$, we obtain

$$\Big(\frac{c}{\overline{\gamma}}\Big)_4 = \Big(\frac{\overline{\gamma}}{c}\Big)_4 = \Big(\frac{c - d\mathsf{i}}{c}\Big)_4 = \Big(\frac{\mathsf{i}}{c}\Big)_4\Big(\frac{-d}{c}\Big)_4 = \Big(\frac{\mathsf{i}}{c}\Big)_4,$$

$$\Big(\frac{a}{\alpha}\Big)_4 = \Big(\frac{\alpha}{a}\Big)_4 = \Big(\frac{a + b\mathsf{i}}{a}\Big)_4 = \Big(\frac{\mathsf{i}}{a}\Big)_4\Big(\frac{b}{a}\Big)_4 = \Big(\frac{\mathsf{i}}{a}\Big)_4$$

and

$$\Big(\frac{ac+bd}{\gamma\overline{\alpha}}\Big)_4 = \Big(\frac{\gamma\overline{\alpha}}{ac+bd}\Big)_4 = \Big(\frac{ac+bd+(ad-bc)\mathsf{i}}{ac+bd}\Big)_4 = \Big(\frac{(ad-bc)\mathsf{i}}{ac+bd}\Big)_4 = \Big(\frac{\mathsf{i}}{ac+bd}\Big)_4.$$

Putting all together, we arrive at

$$\Big(\frac{\alpha}{\gamma}\Big)_4 = \Big(\frac{\gamma}{\alpha}\Big)_4\Big(\frac{\mathsf{i}}{a}\Big)_4\Big(\frac{\mathsf{i}}{c}\Big)_4\Big(\frac{\mathsf{i}}{ac+bd}\Big)_4 = \Big(\frac{\gamma}{\alpha}\Big)_4\Big(\frac{\mathsf{i}}{ac(ac+bd)}\Big)_4 = \Big(\frac{\gamma}{\alpha}\Big)_4(-1)^{bd/4},$$

since $ac(ac+bd) = (ac)^2 + acbd \equiv 1 + bd \bmod 8$.

CASE 2 : $a,\, b,\, c\,, d \in \mathbb{Z}$ are arbitrary, $a \equiv c \equiv 1 \bmod 4$ and $b \equiv d \equiv 0 \bmod 2$. Let $m,\, n \in \mathbb{Z}$ be such that $m \equiv n \equiv 1 \bmod 4$, $|m| = (a, b)$, $|n| = (c, d)$, and set $a = ma_0$, $b = mb_0$, $c = nc_0$, $d = nd_0$, $\alpha_0 = a_0 + b_0\mathsf{i}$ and $\gamma_0 = c_0 + d_0\mathsf{i}$. Then $(a_0, b_0) = (c_0, d_0) = 1$, $a_0 \equiv c_0 \equiv 1 \bmod 4$, $b_0 \equiv d_0 \equiv 0 \bmod 2$, $b_0d_0 \equiv bd \bmod 8$, $\alpha = m\alpha_0$ and $\gamma = n\gamma_0$. By CASE 1 we obtain

$$\begin{aligned}\Big(\frac{\gamma}{\alpha}\Big)_4\Big(\frac{\alpha}{\gamma}\Big)_4^{-1} &= \Big(\frac{n\gamma_0}{m\alpha_0}\Big)_4\Big(\frac{m\alpha_0}{n\gamma_0}\Big)_4^{-1} \\ &= \Big(\frac{n}{m}\Big)_4\Big(\frac{n}{\alpha_0}\Big)_4\Big(\frac{\gamma_0}{m}\Big)_4\Big(\frac{\gamma_0}{\alpha_0}\Big)_4\Big(\frac{m}{n}\Big)_4^{-1}\Big(\frac{m}{\gamma_0}\Big)_4^{-1}\Big(\frac{\alpha_0}{n}\Big)_4^{-1}\Big(\frac{\alpha_0}{\gamma_0}\Big)_4^{-1} \\ &= \Big(\frac{\gamma_0}{\alpha_0}\Big)_4\Big(\frac{\alpha_0}{\gamma_0}\Big)_4^{-1} = (-1)^{b_0d_0/4} = (-1)^{bd/4}\,.\end{aligned}$$

2. If $\alpha \equiv \gamma \equiv 1 \bmod (1+\mathsf{i})^3$, then $b \equiv d \equiv 0 \bmod 2$, $a+b \equiv c+d \equiv 1 \bmod 4$, $\mathcal{N}(\alpha) \equiv 3 - 2a \bmod 16$ and $\mathcal{N}(\gamma) \equiv 3 - 2c \bmod 16$. Hence

$$\frac{\mathcal{N}(\alpha)-1}{4} \equiv \frac{a-1}{2} \bmod 2\,, \quad \frac{\mathcal{N}(\gamma)-1}{4} \equiv \frac{c-1}{2} \bmod 2\,,$$

and if $a - 1 = 4u - b$ and $c - 1 = 4v - d$, where $u,\, v \in \mathbb{Z}$, then it follows that $(a-1)(c-1) = (4u-b)(4v-d) \equiv bd \bmod 8$, and

$$\frac{bd}{4} \equiv \frac{a-1}{2}\,\frac{c-1}{2} \equiv \frac{\mathcal{N}(\alpha)-1}{4}\,\frac{\mathcal{N}(\gamma)-1}{4} \bmod 2\,.$$

Therefore it remains to prove that

$$\Big(\frac{\gamma}{\alpha}\Big)_4\Big(\frac{\alpha}{\gamma}\Big)_4^{-1} = (-1)^{bd/4}\,.$$

Let $e,\, f \in \{\pm 1\}$ be such that $ae \equiv cf \equiv 1 \bmod 4$. By 1. we obtain

$$\begin{aligned}(-1)^{bd/4} = (-1)^{bedf/4} &= \Big(\frac{f\gamma}{e\alpha}\Big)_4\Big(\frac{e\alpha}{f\gamma}\Big)_4^{-1} \\ &= \Big(\frac{f}{e}\Big)_4\Big(\frac{f}{\alpha}\Big)_4\Big(\frac{\gamma}{e}\Big)_4\Big(\frac{\gamma}{\alpha}\Big)_4\Big(\frac{e}{f}\Big)_4^{-1}\Big(\frac{e}{\gamma}\Big)_4^{-1}\Big(\frac{\alpha}{f}\Big)_4^{-1}\Big(\frac{\alpha}{\gamma}\Big)_4^{-1} = \Big(\frac{\gamma}{\alpha}\Big)_4\Big(\frac{\alpha}{\gamma}\Big)_4^{-1}\,. \ \square\end{aligned}$$

Theorem 7.4.8 (Supplement to the biquadratic reciprocity law)**.** *If* $a,\, b \in \mathbb{Z}$ *and* $\alpha = a + b\mathsf{i} \equiv 1 \bmod (1+\mathsf{i})^3$*, then*

$$\Big(\frac{1+\mathsf{i}}{\alpha}\Big)_4 = \mathsf{i}^{(a-b-b^2-1)/4} \quad \text{and} \quad \Big(\frac{2}{\alpha}\Big)_4 = \mathsf{i}^{-b/2}\,.$$

In particular, if $a \in \mathbb{Z}$, $\varepsilon \in \{\pm 1\}$ *and* $a \equiv \varepsilon \bmod 4$*, then*

$$\Big(\frac{1+\mathsf{i}}{a}\Big)_4 = \mathsf{i}^{(a\varepsilon-1)/4}\,.$$

Proof. It suffices to prove the assertions concerning the biquadratic character of $1+\mathsf{i}$, for then

$$\Big(\frac{2}{\alpha}\Big)_4 = \Big(\frac{\mathsf{i}^3(1+\mathsf{i})^2}{\alpha}\Big)_4 = \Big(\frac{\mathsf{i}}{\alpha}\Big)_4^3\Big(\frac{1+\mathsf{i}}{\alpha}\Big)_4^2 = \mathsf{i}^{3(1-a)/2+(a-b-b^2-1)/2} = \mathsf{i}^{-b/2}\,,$$

since $3(1-a) + (a-b-b^2-1) = 2 - 2a - b - b^2 \equiv 2b - b - b^2 \equiv -b \bmod 8\,.$

CASE 1: $\alpha = a \equiv 1 \mod 4$ is a prime. Then $a = \pi\overline{\pi}$ for some prime element $\pi \in D$ such that $\mathcal{N}(\pi) = a$, and therefore we obtain

$$\begin{aligned}\Big(\frac{1+\mathsf{i}}{a}\Big)_4 = \Big(\frac{1+\mathsf{i}}{\pi}\Big)_4\Big(\frac{1+\mathsf{i}}{\overline{\pi}}\Big)_4 &= \Big(\frac{\mathsf{i}}{\pi}\Big)_4\Big(\frac{1-\mathsf{i}}{\pi}\Big)_4\Big(\frac{1+\mathsf{i}}{\overline{\pi}}\Big)_4 \\ &= \Big(\frac{\mathsf{i}}{\pi}\Big)_4\Big(\frac{1-\mathsf{i}}{\pi}\Big)_4\Big(\frac{1-\mathsf{i}}{\pi}\Big)_4^{-1} = \Big(\frac{\mathsf{i}}{\pi}\Big)_4 = \mathsf{i}^{(a-1)/4}\,.\end{aligned}$$

CASE 2: $\alpha = a < 0$ and $q = -a \equiv 3 \mod 4$ is a prime. Then q is a prime element of D, $\mathcal{N}(q) = a^2$, and

$$\Big(\frac{1+\mathsf{i}}{a}\Big)_4 = \Big(\frac{1+\mathsf{i}}{q}\Big)_4 \equiv (1+\mathsf{i})^{(q^2-1)/4} \equiv 2^{(q^2-1)/8}\,\mathsf{i}^{(q^2-1)/8} \mod q\,.$$

Since

$$2^{(q^2-1)/8} = \big(2^{(q-1)/2}\big)^{(q+1)/4} \equiv \Big(\frac{2}{q}\Big)^{(q+1)/4} \equiv (-1)^{[(q+1)/4]^2} \equiv \mathsf{i}^{(q+1)^2/8} \mod q$$

and

$$\frac{(q+1)^2}{8} + \frac{q^2-1}{8} = \frac{(-a+1)^2 + (a^2-1)}{8} = \frac{a^2-a}{4} \equiv \frac{a-1}{4} \mod 4\,,$$

it follows that

$$\Big(\frac{1+\mathsf{i}}{a}\Big)_4 \equiv \mathsf{i}^{(a-1)/4} \mod q\,, \quad \text{and therefore} \quad \Big(\frac{1+\mathsf{i}}{a}\Big)_4 = \mathsf{i}^{(a-1)/4}\,.$$

CASE 3: $a \in \mathbb{Z}$, $\varepsilon \in \{\pm 1\}$ and $a \equiv \varepsilon \mod 4$. Then $a\varepsilon \equiv 1 \mod 4$, and therefore $a\varepsilon = a_1 \cdot \ldots \cdot a_r$, where $r \in \mathbb{N}_0$ and, for all $i \in [1, r]$, $a_i \equiv 1 \mod 4$ and either a_i or $-a_i$ is a prime. By the CASES 1 and 2 we obtain

$$\Big(\frac{1+\mathsf{i}}{a}\Big)_4 = \Big(\frac{1+\mathsf{i}}{a\varepsilon}\Big)_4 = \prod_{i=1}^{r}\Big(\frac{1+\mathsf{i}}{a_i}\Big)_4 = \mathsf{i}^S, \quad \text{where } S = \sum_{i=1}^{r}\frac{a_i-1}{4} \equiv \frac{a\varepsilon-1}{4} \mod 4\,.$$

CASE 4: $a,\, b \in \mathbb{Z}$, $(a, b) = 1$ and $\alpha = a + b\mathsf{i} \equiv 1 \mod (1+\mathsf{i})^3$. Then it follows that $a + b \equiv 1 \mod 4$, $b \equiv 0 \mod 2$, $(a, \alpha) = 1$, $(b, \alpha) = 1$, $(a(1+\mathsf{i}), \alpha) = 1$, $(b(1+\mathsf{i}), \alpha) = 1$, $(a-b, \alpha) = 1$, and we set $a^* = (-1)^{(a-1)/2}a = (-1)^{b/2}a = \mathsf{i}^b a$. By CASE 3, we get

$$\begin{aligned}\Big(\frac{1+\mathsf{i}}{\alpha}\Big)_4 &= \Big(\frac{a}{\alpha}\Big)_4^{-1}\Big(\frac{a+a\mathsf{i}}{a+b\mathsf{i}}\Big)_4 = \Big(\frac{\mathsf{i}^b}{\alpha}\Big)_4\Big(\frac{a^*}{\alpha}\Big)_4^{-1}\Big(\frac{(a-b)\mathsf{i}}{\alpha}\Big)_4 = \Big(\frac{\mathsf{i}}{\alpha}\Big)_4^{b+1}\Big(\frac{\alpha}{a}\Big)_4^{-1}\Big(\frac{\alpha}{a-b}\Big)_4 \\ &= \Big(\frac{\mathsf{i}}{\alpha}\Big)_4^{b+1}\Big(\frac{b\mathsf{i}}{a}\Big)_4^{-1}\Big(\frac{b(1+\mathsf{i})}{a-b}\Big)_4 = \Big(\frac{\mathsf{i}}{\alpha}\Big)_4^{b+1}\Big(\frac{\mathsf{i}}{a}\Big)_4^{-1}\Big(\frac{1+\mathsf{i}}{a-b}\Big)_4 = \mathsf{i}^T\,,\end{aligned}$$

where

$$\begin{aligned}T &= \frac{1-a}{2}\,(b+1) - \frac{1-a^*}{2} + \frac{a-b-1}{4} \\ &\equiv \frac{b^2}{2} + \frac{1-a}{2} - \frac{1-a}{2} + \frac{b^2}{4} + \frac{a-b-1}{4} \equiv \frac{a-b-b^2-1}{4} \mod 4\,,\end{aligned}$$

since $b(1-a) \equiv b^2 \mod 8$, $3b^2 \equiv -b^2 \mod 16$,

$$\frac{b^2}{4} \equiv \begin{cases} 1 \mod 4 & \text{if} \quad b \equiv 2 \mod 4\,, \\ 0 \mod 4 & \text{if} \quad b \equiv 0 \mod 4\,, \end{cases} \quad \text{and thus} \quad \frac{1-a^*}{2} \equiv \frac{1-a}{2} - \frac{b^2}{4} \mod 4\,.$$

CASE 5: $a,\ b \in \mathbb{Z}$ and $\alpha = a + b\mathrm{i} \equiv 1 \bmod (1+\mathrm{i})^3$. Let $d \in \mathbb{Z}$ be such that $d \equiv 1 \bmod 4,\ \ |d| = (a,b),\ \ a = da_0,\ \ b = db_0$ and $\alpha = d\alpha_0$, whence $(a_0, b_0) = 1$ and $\alpha_0 = a_0 + b_0\mathrm{i} \equiv 1 \bmod (1+\mathrm{i})^3$. By the CASES 3 and 4, we get

$$\Big(\frac{1+\mathrm{i}}{\alpha}\Big)_4 = \Big(\frac{1+\mathrm{i}}{d}\Big)_4 \Big(\frac{1+\mathrm{i}}{\alpha_0}\Big)_4 = \mathrm{i}^{(d-1)/4 + (a_0 - b_0 - b_0^2 - 1)/4}\,.$$

Since $b_0 \equiv 0 \bmod 2$ and $d \equiv 1 \bmod 4$, we obtain $b^2 = b_0^2 d^2 \equiv b_0^2 d \bmod 16$, and therefore

$$\frac{d-1}{4} + \frac{a_0 - b_0 - b_0^2 - 1}{4} \equiv \frac{d(a_0 - b_0 - b_0^2) - 1}{4} \equiv \frac{a - b - b^2 - 1}{4} \bmod 4\,. \qquad \square$$

Exercise 7.4.9. Suppose that $a,\ b \in \mathbb{Z}$ and $\alpha = a + b\mathrm{i} \equiv 1 \bmod 2$. Prove that

$$\Big(\frac{2}{\alpha}\Big)_4 = \mathrm{i}^{-(a+b)b/2}\,.$$

Exercise 7.4.10. Calculate the biquadratic Jacobi symbols

$$\Big(\frac{3+10\mathrm{i}}{7+2\mathrm{i}}\Big)_4, \quad \Big(\frac{-9+7\mathrm{i}}{7+12\mathrm{i}}\Big)_4 \quad \text{and} \quad \Big(\frac{5+2\mathrm{i}}{-2-7\mathrm{i}}\Big)_4\,.$$

Hint: Use the division algorithm in D: For any $\alpha,\ \beta \in D^\bullet$, there exist $\gamma,\ \delta \in D$ such that $\alpha = \beta\gamma + \delta$ and $\mathcal{N}(\delta) < \mathcal{N}(\beta)$.

Theorem 7.4.11 (Quadratic reciprocity law in D)**.** *Let* $\alpha,\ \gamma \in D$ *be such that* $\alpha \equiv \gamma \equiv 1 \bmod 2,\ \ (\alpha,\gamma) = 1,\ \ \alpha = a + b\mathrm{i}$, *where* $a,\ b \in \mathbb{Z}$ *and* $\varepsilon \in \{\pm 1\}$ *such that* $a + b \equiv \varepsilon \bmod 4$. *Then*

$$\Big(\frac{\mathrm{i}}{\alpha}\Big)_2 = (-1)^{b/2}, \quad \Big(\frac{1+\mathrm{i}}{\alpha}\Big)_2 = (-1)^{(a+b-\varepsilon)/4} \quad \textit{and} \quad \Big(\frac{\gamma}{\alpha}\Big)_2 = \Big(\frac{\alpha}{\gamma}\Big)_2\,.$$

PROOF. By assumption, $b \equiv 0 \bmod 2$, $\varepsilon\alpha = \varepsilon a + \varepsilon b\mathrm{i} \equiv 1 \bmod (1+\mathrm{i})^3$, and there exists some $\eta \in \{\pm 1\}$ such that $\eta\beta \equiv 1 \bmod (1+\mathrm{i})^3$. Hence we obtain

$$\Big(\frac{\mathrm{i}}{\alpha}\Big)_2 = \Big(\frac{\mathrm{i}}{\alpha}\Big)_4^2 = \Big(\frac{-1}{\alpha}\Big)_4,$$

and since $\varepsilon a - \varepsilon b - b^2 - 1 \equiv a + b - \varepsilon \bmod 8$, it follows that

$$\Big(\frac{1+\mathrm{i}}{\alpha}\Big)_2 = \Big(\frac{1+\mathrm{i}}{\varepsilon\alpha}\Big)_4^2 = (-1)^{(\varepsilon a - \varepsilon b - b^2 - 1)/4} = (-1)^{(a+b-\varepsilon)/4}\,.$$

Finally, since

$$\Big(\frac{-1}{\alpha}\Big)_2 = \Big(\frac{-1}{\gamma}\Big)_2 = 1\,, \quad \text{we get} \quad \Big(\frac{\eta}{\varepsilon\alpha}\Big)_2 = \Big(\frac{\varepsilon}{\eta\gamma}\Big)_2 = 1\,,$$

and the biquadratic reciprocity law yields

$$\Big(\frac{\gamma}{\alpha}\Big)_2 = \Big(\frac{\gamma}{\varepsilon\alpha}\Big)_2 \Big(\frac{\eta}{\varepsilon\alpha}\Big)_2 = \Big(\frac{\eta\gamma}{\varepsilon\alpha}\Big)_2 = \Big(\frac{\varepsilon\alpha}{\eta\gamma}\Big)_2 = \Big(\frac{\varepsilon}{\eta\gamma}\Big)_2 \Big(\frac{\alpha}{\eta\gamma}\Big)_2 = \Big(\frac{\alpha}{\gamma}\Big)_2\,. \qquad \square$$

We end this section with some reciprocity formulas which connect the weak biquadratic reciprocity law with the quadratic reciprocity law in D and certain rational Jacobi symbols. These formulas embody a first step towards the purely rational reciprocity laws which we will consider in the following section.

Theorem 7.4.12. *Suppose that* $\mu = a+b\mathsf{i}$, $\nu = c+d\mathsf{i}$, $m=a^2+b^2$ *and* $n=c^2+d^2$, *where* $a,\,b,\,c,\,d\in\mathbb{Z}$ *and* $(a,b)=(c,d)=(m,n)=1$. *Then*

$$\Big(\frac{\nu}{\mu}\Big)_2 = \Big(\frac{ac+bd}{m}\Big) = \Big(\frac{n}{m}\Big)\Big(\frac{ac-bd}{m}\Big)$$
$$= (-1)^{(m-1)/4}\Big(\frac{ad-bc}{m}\Big) = (-1)^{(m-1)/4}\Big(\frac{n}{m}\Big)\Big(\frac{ad+bc}{m}\Big),$$

$$\Big(\frac{m}{\nu}\Big)_4 = \Big(\frac{n}{\mu}\Big)_4\Big(\frac{\overline{\nu}}{\mu}\Big)_2 \quad \textit{and} \quad \Big(\frac{m}{\nu}\Big)_4\Big(\frac{n}{\mu}\Big)_4 = \Big(\frac{\nu}{\mu}\Big)_2 .$$

Proof. By the Theorems 7.3.9.1 and 3.4.5 we obtain

$$\Big(\frac{k}{\mu}\Big)_2 = \Big(\frac{k}{m}\Big) \quad \text{for all } k\in\mathbb{Z}, \quad \Big(\frac{-1}{m}\Big) = \Big(\frac{a}{m}\Big) = 1 \quad \text{and} \quad \Big(\frac{b}{m}\Big) = (-1)^{(m-1)/4} .$$

Since $(a,m)=(b,n)=1$, $ad\mathsf{i}\equiv bd \bmod \mu$ and $bd\mathsf{i}\equiv -ad \bmod \mu$, it follows that

$$\Big(\frac{\nu}{\mu}\Big)_2 = \Big(\frac{a}{\mu}\Big)_2\Big(\frac{ac+ad\mathsf{i}}{\mu}\Big)_2 = \Big(\frac{a}{m}\Big)\Big(\frac{ac+bd}{\mu}\Big)_2 = \Big(\frac{ac+bd}{m}\Big)$$
$$= \Big(\frac{b}{\mu}\Big)_2\Big(\frac{bc+bd\mathsf{i}}{\mu}\Big)_2 = \Big(\frac{b}{m}\Big)\Big(\frac{bc-ad}{\mu}\Big)_2 = (-1)^{(m-1)/4}\Big(\frac{ad-bc}{m}\Big).$$

If we replace d by $-d$, we obtain

$$\Big(\frac{\overline{\nu}}{\mu}\Big)_2 = \Big(\frac{ac-bd}{m}\Big) = (-1)^{(m-1)/4}\Big(\frac{-ad-bc}{m}\Big) = (-1)^{(m-1)/4}\Big(\frac{ad+bc}{m}\Big)$$

and

$$\Big(\frac{n}{m}\Big) = \Big(\frac{n}{\mu}\Big)_2 = \Big(\frac{\nu}{\mu}\Big)_2\Big(\frac{\overline{\nu}}{\mu}\Big)_2 = \Big(\frac{ac+bd}{m}\Big)\Big(\frac{ac-bd}{m}\Big) = \Big(\frac{ad-bc}{m}\Big)\Big(\frac{ad+bc}{m}\Big).$$

Hence it follows that

$$\Big(\frac{ac+bd}{m}\Big) = \Big(\frac{n}{m}\Big)\Big(\frac{ac-bd}{m}\Big) \quad \text{and} \quad \Big(\frac{ad-bc}{m}\Big) = \Big(\frac{n}{m}\Big)\Big(\frac{ad+bc}{m}\Big).$$

By the weak biquadratic reciprocity law we obtain

$$\Big(\frac{m}{\nu}\Big)_4 = \Big(\frac{\nu}{m}\Big)_4 = \Big(\frac{\nu}{\mu}\Big)_4\Big(\frac{\nu}{\overline{\mu}}\Big)_4 = \Big(\frac{\nu}{\mu}\Big)_4\Big(\frac{\overline{\nu}}{\mu}\Big)_4^3 = \Big(\frac{n}{\mu}\Big)_4\Big(\frac{\overline{\nu}}{\mu}\Big)_2,$$

and therefore

$$\Big(\frac{m}{\nu}\Big)_4\Big(\frac{n}{\mu}\Big)_4 = \Big(\frac{n}{\mu}\Big)_4^2\Big(\frac{\overline{\nu}}{\mu}\Big)_2 = \Big(\frac{n\overline{\nu}}{\mu}\Big)_2 = \Big(\frac{\nu\overline{\nu}^2}{\mu}\Big)_2 = \Big(\frac{\nu}{\mu}\Big)_2 . \qquad \square$$

7.5. Rational biquadratic reciprocity laws

In the previous section we have derived the general biquadratic reciprocity law in $D = \mathbb{Z}[\mathrm{i}]$, and now we come back to the original topic of classical number theory, the ordinary integers. Modeled on the definition of the Legendre symbol for quadratic residues, we define a rational biquadratic residue symbol and investigate its properties. The main results of this section are the reciprocity laws for this rational biquadratic residue symbol and its connections with the quadratic residue character of certain quadratic irrationals. Although many basic ideas go back to Dirichlet, the major part of the investigations on rational biquadratic reciprocity laws was done in the second half of the 20th century.

Let p be an odd prime and $a \in \mathbb{Z} \setminus p\mathbb{Z}$ a quadratic residue modulo p. Then we define the *rational biquadratic residue symbol* modulo p by

$$\Big[\frac{a}{p}\Big]_4 = \begin{cases} 1 & \text{if } a \text{ is a biquadratic residue modulo } p\,, \\ -1 & \text{otherwise.} \end{cases}$$

By definition, this symbol depends only on the residue class $a + p\mathbb{Z} \in \mathbb{F}_p$.

If $a \in \mathbb{Z} \setminus p\mathbb{Z}$, then Theorem 3.1.2.2 implies that a is a biquadratic residue modulo p if and only if $a^{(p-1)/(4,p-1)} \equiv 1 \bmod p$. If $p \equiv 3 \bmod 4$, then

$$\Big(\frac{a}{p}\Big) = 1 \quad \text{implies} \quad \Big[\frac{a}{p}\Big]_4 = 1 = \Big(\frac{a}{p}\Big)_4 \qquad \text{(by Theorem 7.3.5.3).}$$

If $p \equiv 1 \bmod 4$, then $p = \pi\overline{\pi}$ for some prime element $\pi \in D$ such that $\mathcal{N}(\pi) = p$,

$$\Big(\frac{a}{p}\Big) = 1 \quad \text{implies} \quad \Big[\frac{a}{p}\Big]_4 \equiv a^{(p-1)/4} \bmod p\,, \quad \text{hence} \quad \Big[\frac{a}{p}\Big]_4 \equiv a^{(p-1)/4} \bmod \pi\,,$$

and therefore

$$\Big[\frac{a}{p}\Big]_4 = \Big(\frac{a}{\pi}\Big)_4\,.$$

As before, we extend this definition multiplicatively and define the *rational biquadratic Jacobi symbol* as follows. Suppose that $m = p_1 \cdot \ldots \cdot p_r$, where $r \in \mathbb{N}_0$ and $p_1, \ldots, p_r$ are primes. If $a \in \mathbb{Z}$, $(a,m) = 1$ and a is a quadratic residue modulo m, then $a \in \mathbb{Z} \setminus p_i\mathbb{Z}$, a is a quadratic residue modulo p_i for all $i \in [1,r]$, and we define

$$\Big[\frac{a}{m}\Big]_4 = \prod_{i=1}^{r} \Big[\frac{a}{p_i}\Big]_4\,.$$

In the following Theorem 7.5.1 we collect elementary properties of the rational biquadratic Jacobi symbol. Recall from Theorem 6.2.6 that, if a positive integer m is a product of primes $p \equiv 1 \bmod 4$, then it is a sum of two integral squares, and if m is a product of primes $p \equiv 1 \bmod 8$, then $m = c^2 + 2d^2$ for some c, $d \in \mathbb{N}$.

Theorem 7.5.1. *Let $m \in \mathbb{N}$ be odd.*

1. *Suppose that $m = m_1m_2$, where m_1, $m_2 \in \mathbb{N}$. Let a, b, $c \in \mathbb{Z}$ be coprime to m, and let a and b be quadratic residues modulo m. Then*

$$\Big[\frac{a}{m_1m_2}\Big]_4 = \Big[\frac{a}{m_1}\Big]_4\Big[\frac{a}{m_2}\Big]_4, \quad \Big[\frac{ab}{m}\Big]_4 = \Big[\frac{a}{m}\Big]_4\Big[\frac{b}{m}\Big]_4, \quad \Big[\frac{c^2}{m}\Big]_4 = \Big(\frac{c}{m}\Big),$$

and if $a \equiv b \bmod m$, *then*

$$\Big[\frac{a}{m}\Big]_4 = \Big[\frac{b}{m}\Big]_4 .$$

2. *Let* m *be a product of primes* $p \equiv 1 \bmod 4$, $m = a^2 + b^2$, *where* $a, b \in \mathbb{N}$, $(a,b) = 1$, $2 \,|\, b$ *and* $\alpha = a + b\mathsf{i}$.
   (a) *If* $a \in \mathbb{Z}$, $(a,m) = 1$, *and* a *is a quadratic residue modulo* m, *then*
   $$\Big[\frac{a}{m}\Big]_4 = \Big(\frac{a}{\alpha}\Big)_4 , \quad \textit{and} \quad \Big[\frac{-1}{m}\Big]_4 = \Big(\frac{2}{m}\Big) = (-1)^{b/2} .$$
   (b) *Let* m *be a product of primes* $p \equiv 1 \bmod 8$. *Then* $4 \,|\, b$, $m = c^2 + 2d^2$ *for some* c, $d \in \mathbb{N}$ *such that* $2 \,|\, d$, *and*
   $$\Big[\frac{2}{m}\Big]_4 = (-1)^{b/4} = (-1)^{n+d/2} .$$

Proof. 1. If a is a quadratic residue modulo m, then a is a quadratic residue modulo m_1 and modulo m_2, and the first equality holds by the very definition. For the other two, it suffices to consider the case where $m = p$ is an odd prime, and there is nothing to do if $p \equiv 3 \bmod 4$. If $p \equiv 1 \bmod 4$ and $\pi \in D$ is such that $\mathcal{N}(\pi) = p$, then

$$\Big[\frac{ab}{p}\Big]_4 = \Big(\frac{ab}{\pi}\Big)_4 = \Big(\frac{a}{\pi}\Big)_4 \Big(\frac{b}{\pi}\Big)_4 = \Big[\frac{a}{p}\Big]_4 \Big[\frac{b}{p}\Big]_4 ,$$

and as c^2 is a quadratic residue modulo p, we obtain

$$\Big[\frac{c^2}{p}\Big]_4 \equiv (c^2)^{(p-1)/4} \equiv c^{(p-1)/2} \equiv \Big(\frac{c}{p}\Big) \mod p ,$$

and thus equality holds.

If $a \equiv b \bmod m$, then $a \equiv b \bmod p$ for all primes p dividing m, and therefore

$$\Big[\frac{a}{m}\Big]_4 = \Big[\frac{b}{m}\Big]_4 .$$

2. There is a factorization $\alpha = a + b\mathsf{i} = \pi_1 \cdot \ldots \cdot \pi_s$, where $s \in \mathbb{N}$ and $\pi_1, \ldots, \pi_s$ are prime elements of D. Then it follows that $m = \mathcal{N}(\alpha) = p_1 \cdot \ldots \cdot p_r$ with primes $p_i = \mathcal{N}(\pi_i) \equiv 1 \bmod 4$.

(a) By definition,

$$\Big[\frac{a}{m}\Big]_4 = \prod_{i=1}^{r} \Big[\frac{a}{p_i}\Big]_4 = \prod_{i=1}^{r} \Big(\frac{a}{\pi_i}\Big)_4 = \Big(\frac{a}{\alpha}\Big)_4 ,$$

and therefore, by Theorem 7.3.8,

$$\Big[\frac{-1}{m}\Big]_4 = \Big(\frac{-1}{\alpha}\Big)_4 = (-1)^{b/2} = \Big(\frac{2}{m}\Big) = (-1)^{(m-1)/4} .$$

(b) As m is a product of primes $p \equiv 1 \bmod 8$, it follows that $b \equiv 0 \bmod 4$ and 2 is a quadratic residue modulo m. Replacing a by $-a$ if necessary, we may assume that $a \equiv 1 \bmod 4$, hence $\alpha \equiv 1 \bmod (1+\mathsf{i})^3$, and therefore, using Theorem 6.2.6.4(a),

$$\Big[\frac{2}{m}\Big]_4 = \Big(\frac{2}{\mu}\Big)_4 = \mathsf{i}^{-b/2} = (-1)^{b/4} = (-1)^{n+d/2} . \qquad \square$$

Exercise 7.5.2. Let m be a product of primes $p \equiv 1 \bmod 8$, and suppose that $m = a^2 + b^2$, where $b \equiv 0 \bmod 4$. Prove that there exist positive integers c, d, e, f, n such that $m = c^2 + 2d^2 = e^2 - 2f^2 = 8n + 1$, and for any choice of c, d, e, f, n with these properties we have

$$\Big[\frac{2}{m}\Big]_4 = (-1)^{b/4} = (-1)^{n+d/2} = \Big(\frac{2}{c}\Big) = \Big(\frac{-2}{e}\Big)\,.$$

Hint: Use Theorem 6.2.6, and observe that $\mathbb{Z}[\sqrt{2}\,]$ and $\mathbb{Z}[\sqrt{-2}\,]$ are principal ideal domains.

One of the main properties of the rational biquadratic Jacobi symbol is its connection with the quadratic residue character of certain quadratic irrationals. For this we introduce the following notations.

Let $m \in \mathbb{N}$ be odd, $a \in \mathbb{Z}$ not a square, $\alpha = u + v\sqrt{a} \in \mathbb{Z}[\sqrt{a}\,]$, where u, $v \in \mathbb{Z}$, and $\mathcal{N}(\alpha) = u^2 - v^2a$. Suppose that $(a, m) = (\mathcal{N}(\alpha), m) = 1$, and that both a and $\mathcal{N}(\alpha)$ are quadratic residues modulo m. If $t \in \mathbb{Z}$ and $t^2 \equiv a \bmod m$, then $(u + vt)(u - vt) \equiv u^2 - v^2t^2 \equiv \mathcal{N}(\alpha) \bmod m$, hence $(u + vt, m) = 1$, and we define a *generalized quadratic Jacobi symbol* by

$$\Big(\frac{\alpha}{m}\Big) = \Big(\frac{u + v\sqrt{a}}{m}\Big) = \Big(\frac{u + vt}{m}\Big) \in \{\pm 1\}\,.$$

We assert that this definition does not depend on the choice of t. Indeed, suppose that t, $t_1 \in \mathbb{Z}$ are such that $t^2 \equiv t_1^2 \equiv a \bmod m$, and $m = q_1 \cdot \ldots \cdot q_r$, where $r \in \mathbb{N}_0$ and $q_1, \ldots, q_r$ are odd primes. Then it suffices to prove that

$$\Big(\frac{u + vt}{q_i}\Big) = \Big(\frac{u + vt_1}{q_i}\Big) \quad \text{for all} \ \ i \in [1, r]\,.$$

If $i \in [1, r]$, then $t_1^2 \equiv t^2 \bmod q_i$, and we may assume that $t_1 \not\equiv t \bmod q_i$. Then $t_1 \equiv -t \bmod q_i$, $u^2 - v^2a \equiv (u + vt)(u + vt_1) \bmod q_i$, hence

$$1 = \Big(\frac{u^2 - v^2a}{q_i}\Big) = \Big(\frac{u + vt}{q_i}\Big)\Big(\frac{u + vt_1}{q_i}\Big), \quad \text{and therefore} \quad \Big(\frac{u + vt}{q_i}\Big) = \Big(\frac{u + vt_1}{q_i}\Big)\,.$$

In particular, it follows that

$$\Big(\frac{u + vt}{m}\Big) = \Big(\frac{u - vt}{m}\Big), \quad \text{and} \quad \Big(\frac{\sqrt{a}}{m}\Big) = \Big(\frac{t}{m}\Big) = \Big[\frac{t^2}{m}\Big]_4 = \Big[\frac{a}{m}\Big]_4\,.$$

Suppose that α_1, $\alpha_2 \in \mathbb{Z}[\sqrt{a}\,]$ are such that both $\mathcal{N}(\alpha_1)$ and $\mathcal{N}(\alpha_2)$ are coprime to m and quadratic residues modulo m. Then $\mathcal{N}(\alpha_1\alpha_2) = \mathcal{N}(\alpha_1)\mathcal{N}(\alpha_2)$ is coprime to m, it is a quadratic residue modulo m, and we assert that

$$\Big(\frac{\alpha_1\alpha_2}{m}\Big) = \Big(\frac{\alpha_1}{m}\Big)\Big(\frac{\alpha_2}{m}\Big)\,.$$

Indeed, let $t \in \mathbb{Z}$ be such that $t^2 \equiv a \bmod m$, and for $i \in \{1, 2\}$ let u_i, $v_i \in \mathbb{Z}$ be such that $\alpha_i = u_i + v_i\sqrt{a}$. Then $\alpha_1\alpha_2 = (u_1u_2 + v_1v_2a) + (u_1v_+u_2v_1)\sqrt{a}$, and since $u_1u_2 + v_1v_2a + (u_1v_2 + u_2v_1)t \equiv (u_1 + v_1t)(u_2 + v_2t) \bmod m$, we get

$$\begin{aligned}\Big(\frac{\alpha_1\alpha_2}{m}\Big) &= \Big(\frac{u_1u_2 + v_1v_2a + (u_1v_2 + u_2v_1)t}{m}\Big) = \Big(\frac{u_1 + v_1t}{m}\Big)\Big(\frac{u_2 + v_2t}{m}\Big) \\ &= \Big(\frac{\alpha_1}{m}\Big)\Big(\frac{\alpha_2}{m}\Big)\,.\end{aligned}$$

If $m=p$ is an odd prime, then

$$\mathsf{Q}_{4a}(p)=\Big(\frac{4a}{p}\Big)=1\,,$$

and as $\mathbb{Z}[\sqrt{a}\,]=\mathcal{O}_{4a}$, it follows by Theorem 5.8.8.1 that $p\mathbb{Z}[\sqrt{a}\,]=\mathfrak{p}\mathfrak{p}'$, where $\mathfrak{p}$, $\mathfrak{p}'$ are prime ideals of $\mathbb{Z}[\sqrt{a}\,]$ such that $\mathfrak{p}\ne\mathfrak{p}'$ and $\mathfrak{N}_{4a}(\mathfrak{p})=\mathfrak{N}_{4a}(\mathfrak{p}')=p$. We consider the isomorphisms $\iota_\mathfrak{p}\colon\mathbb{Z}/p\mathbb{Z}\to\mathbb{Z}[\sqrt{a}\,]/\mathfrak{p}$ and $\iota_{\mathfrak{p}'}\colon\mathbb{Z}/p\mathbb{Z}\to\mathbb{Z}[\sqrt{a}\,]/\mathfrak{p}'$, defined by $\iota(c+p\mathbb{Z})=c+\mathfrak{p}$ and $\iota'(c+p\mathbb{Z})=c+\mathfrak{p}'$ for all $c\in\mathbb{Z}$. By interchanging $\mathfrak{p}$ and $\mathfrak{p}'$ (if necessary) we may assume that $\iota_\mathfrak{p}(t+p\mathbb{Z})=\sqrt{a}+\mathfrak{p}$ and $\iota_{\mathfrak{p}'}(t+p\mathbb{Z})=-\sqrt{a}+\mathfrak{p}'$. Then it follows that $\iota_\mathfrak{p}(u+vt+p\mathbb{Z})=\alpha+\mathfrak{p}$ and $\iota_{\mathfrak{p}'}(u-vt+p\mathbb{Z})=\alpha+\mathfrak{p}'$, and by the Chinese remainder theorem, we obtain an isomorphism

$$\theta\colon\mathbb{Z}[\sqrt{a}\,]/p\mathbb{Z}[\sqrt{a}\,]\ \overset{\sim}{\to}\ \mathbb{Z}[\sqrt{a}\,]/\mathfrak{p}\times\mathbb{Z}[\sqrt{a}\,]/\mathfrak{p}'\ \overset{\gamma}{\to}\ \mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$$

(where $\gamma=(\iota_\mathfrak{p},\iota_{\mathfrak{p}'})^{-1}$) such that $\theta(\alpha+p\mathbb{Z}[\sqrt{a}\,]=(u+vt+p\mathbb{Z},u-vt+p\mathbb{Z})$. Hence

$$\Big(\frac{\alpha}{p}\Big)=1\quad\text{if and only if}\quad\alpha+p\mathbb{Z}[\sqrt{a}\,]\ \text{ is a square in }\ \mathbb{Z}[\sqrt{a}\,]/p\mathbb{Z}[\sqrt{a}\,]\,.$$

In this case we call α a *quadratic residue* modulo p.

Occasionally we shall use both the rational biquadratic Jacobi symbol and the generalized quadratic Jacobi symbol for fractional arguments as follows (compare Theorem and Definition A.8.5).

Let $m\in\mathbb{N}$ be odd. If $z=c^{-1}a\in\mathbb{Z}_{[m]}^\times$, where a, $c\in\mathbb{Z}$ and $(a,c)=(a,m)=1$, then there exists some $d\in\mathbb{Z}$ such that $cd\equiv1\bmod m$, and if both a and c are quadratic residues modulo m, then d is also a quadratic residue modulo m, and $z+m\mathbb{Z}_{[m]}$ is a square in $\mathbb{Z}_{[m]}/m\mathbb{Z}_{[m]}=\mathbb{Z}/m\mathbb{Z}$. In this case, we set

$$\Big[\frac{z}{m}\Big]_4=\Big[\frac{da}{m}\Big]_4$$

(which obviously only depends on z and m, and not on a, c and d).

We can do the same for the generalized quadratic Jacobi symbol. Assume that $a\in\mathbb{Z}$ is not a square, $\alpha=u+v\sqrt{a}\in\mathbb{Z}[\sqrt{a}\,]$, where u, $v\in\mathbb{Z}$, and $\mathcal{N}(\alpha)=u^2-v^2a$. Suppose that $(a,m)=(\mathcal{N}(\alpha),m)=1$, and that both a and $\mathcal{N}(\alpha)$ are quadratic residues modulo m. If $c\in\mathbb{Z}$ and $(c,m)=1$, then $z=c^{-1}\alpha\in\mathbb{Z}[\sqrt{a}\,]_{[m]}$, and we define

$$\Big(\frac{z}{m}\Big)=\Big(\frac{c}{m}\Big)\Big(\frac{\alpha}{m}\Big)$$

(which obviously only depends on z and m, and not on α and c).

In the following theorem, we gather results which (in the special case where m and n are primes) were proved by K. Burde [**15**] and partially go back to Dirichlet.

Theorem 7.5.3 (Dirichlet, Burde)**.** *Let $m,\,n\in\mathbb{N}$ be odd, $m=a^2+b^2$ and $n=c^2+d^2$, where $a,\,b,\,c,\,d\in\mathbb{N}$, $2\nmid ac$, and $(a,b)=(c,d)=(m,n)=1$. Suppose that m is a quadratic residue modulo n, and n is a quadratic residue modulo m.*

Then

$$\Big[\frac{m}{n}\Big]_4\Big[\frac{n}{m}\Big]_4=\Big(\frac{c+d\mathrm{i}}{m}\Big)=\Big(\frac{ac+bd}{m}\Big)=\Big(\frac{ac-bd}{m}\Big)=\Big(\frac{d+\sqrt{n}}{m}\Big)$$
$$=(-1)^{(m-1)/4}\Big(\frac{ad-bc}{m}\Big)=(-1)^{(m-1)/4}\Big(\frac{ad+bc}{m}\Big)=\Big(\frac{2}{m}\Big)\Big(\frac{c+\sqrt{n}}{m}\Big).$$

Proof. By Theorem 3.4.1, both m and n are products of primes $p\equiv 1 \bmod 4$, and as they are reciprocally quadratic residues, it follows that

$$\Big(\frac{m}{n}\Big)=\Big(\frac{n}{m}\Big)=1\,.$$

If $\mu=a+b\mathrm{i}$ and $\nu=c+d\mathrm{i}$, then Theorem 7.4.12 implies

$$\Big[\frac{m}{n}\Big]_4\Big[\frac{n}{m}\Big]_4=\Big(\frac{m}{\nu}\Big)_4\Big(\frac{n}{\mu}\Big)_4=\Big(\frac{\nu}{\mu}\Big)_2=\Big(\frac{ac+bd}{m}\Big)=\Big(\frac{ac-bd}{m}\Big)$$
$$=(-1)^{(m-1)/4}\Big(\frac{ad-bc}{m}\Big)=(-1)^{(m-1)/4}\Big(\frac{ad+bc}{m}\Big).$$

Let $e,\,s\in\mathbb{Z}$ be such that $e^2\equiv -1 \bmod m$ and $s^2\equiv n \bmod m$. Since $\mathcal{N}(c+d\mathrm{i})=n$ and $\mathcal{N}(d+\sqrt{n})=-c^2$ are quadratic residues modulo m, we obtain (using Theorem 7.3.9.1 and the definition of the generalized quadratic Jacobi symbol)

$$\Big(\frac{\nu}{\mu}\Big)_2=\Big(\frac{c+d\mathrm{i}}{\mu}\Big)_2=\Big(\frac{c+de}{\mu}\Big)_2=\Big(\frac{c+de}{m}\Big)=\Big(\frac{c+d\mathrm{i}}{m}\Big),$$

$$\Big(\frac{c+\sqrt{n}}{m}\Big)=\Big(\frac{c+s}{m}\Big)\quad\text{and}\quad\Big(\frac{d+\sqrt{n}}{m}\Big)=\Big(\frac{d+s}{m}\Big).$$

From the congruences

$$(c+d+s)^2\equiv 2(c+s)(d+s) \bmod m\quad\text{and}\quad(c+de+s)^2\equiv 2(c+s)(c+de) \bmod m$$

we obtain

$$1=\Big(\frac{2}{m}\Big)\Big(\frac{c+s}{m}\Big)\Big(\frac{d+s}{m}\Big)=\Big(\frac{2}{m}\Big)\Big(\frac{c+s}{m}\Big)\Big(\frac{c+de}{m}\Big),$$

and thus finally

$$\Big(\frac{c{+}d\mathrm{i}}{m}\Big)=\Big(\frac{c{+}de}{m}\Big)=\Big(\frac{2}{m}\Big)\Big(\frac{c{+}s}{m}\Big)=\Big(\frac{d{+}s}{m}\Big)=\Big(\frac{2}{m}\Big)\Big(\frac{c+\sqrt{n}}{m}\Big)=\Big(\frac{d+\sqrt{n}}{m}\Big).\ \square$$

In the following theorem, we present the reciprocity law of H. C. Williams, K. Hardy and C. Friesen which seems to be the most general rational biquadratic reciprocity law. In particular, it contains as special cases the rational biquadratic reciprocity laws by E. Lehmer (Theorem 7.5.9), T. Schönemann and A. Scholz (Corollary 7.5.7), and K. Burde (Theorem 7.5.3). Our proof is modeled after the original proof given in [**50**], but we remark that there is a more structural proof using class field theory by F. Lemmermeyer; see [**67**, Sec. 5.4] and the references given there. Chapter 5 of Lemmermeyer's book [**67**] contains a wealth of further results and historical remarks and is warmly recommended to an interested reader.

Theorem 7.5.4 (Williams, Hardy, Friesen). *Assume that* $m = 2^\delta m_0 > 1$ *for some* $\delta \in \{0,1\}$ *and* $m_0 = p_1 \cdot \ldots \cdot p_r > 1$, *where* $r \in \mathbb{N}_0$ *and* $p_1, \ldots, p_r$ *are distinct primes such that* $p_i \equiv 1 \bmod 4$ *for all* $i \in [1, r]$. *Let* q *be an odd prime,* $q^* = (-1)^{(q-1)/2} q$, *and let* A, B, $C \in \mathbb{N}$ *be such that* $(A,B) = (B,C) = (C,A) = 1$. *Suppose that*

$$A^2 = m(B^2+C^2)\,, \quad \Big(\frac{2}{q}\Big)^\delta = 1 \quad \text{and} \quad \Big(\frac{p_i}{q}\Big) = 1 \quad \text{for all } i \in [1,r]\,.$$

1. *If* $\delta = 0$, *then* $m \equiv 1 \bmod 4$, *and*
$$\Big(\frac{A+B\sqrt{m}}{q}\Big) = \Big(\frac{2}{q}\Big)^B \Big[\frac{q^*}{m}\Big]_4 .$$
2. *If* $\delta = 1$, *then* $m = 2m_0 \equiv 2 \bmod 8$, $q \equiv \varepsilon \bmod 8$ *for some* $\varepsilon \in \{\pm 1\}$, *and*
$$\Big(\frac{A+B\sqrt{m}}{q}\Big) = (-1)^{(q-\varepsilon)/8} \Big[\frac{q^*}{m_0}\Big]_4 .$$

PROOF. Throughout the proof, we shall tacitly use the quadratic reciprocity law and the properties of the quadratic and biquadratic symbols.

If $\delta = 1$, then $m = 2m_0 \equiv 2 \bmod 8$, $(B,C) = 1$ implies $A \equiv 2 \bmod 4$, and

$$\Big(\frac{2}{q}\Big) = 1 \quad \text{implies} \quad q \equiv \varepsilon \bmod 8 \quad \text{for some} \quad \varepsilon \in \{\pm 1\}\,.$$

Since

$$\Big(\frac{q}{p_i}\Big) = \Big(\frac{q^*}{p_i}\Big) = \Big(\frac{p_i}{q}\Big) = 1 \quad \text{for all } i \in [1,r],$$

it follows that $q \nmid m$, q and q^* are quadratic residues modulo m, and the rational biquadratic residue symbols in question are defined.

Since $\mathcal{N}(A+B\sqrt{m}) = A^2 - B^2 m = mC^2$ and

$$\Big(\frac{mC^2}{q}\Big) = \Big(\frac{m}{q}\Big) = \Big(\frac{2}{q}\Big)^\delta \prod_{i=1}^r \Big(\frac{p_i}{q}\Big) = 1\,, \quad \text{the symbol} \quad \Big(\frac{A+B\sqrt{m}}{q}\Big) \quad \text{is defined.}$$

Since m is squarefree, we obtain $A = ma$ for some $a \in \mathbb{N}$, hence $ma^2 = B^2 + C^2$, and $(a,B) = (a,C) = (m,B) = (m,C) = 1$. Moreover, $(B,C) = 1$ implies $2 \nmid a$.

From the identity $2(A+B\sqrt{m}\,)(A+C\sqrt{m}\,) = [A + (B+C)\sqrt{m}\,]^2$ we obtain

$$\Big(\frac{A+B\sqrt{m}}{q}\Big) = \Big(\frac{2}{q}\Big)\Big(\frac{A+C\sqrt{m}}{q}\Big),$$

which shows that the assertion of the theorem is symmetric in B and C.

CASE **A.** $q \nmid BC$. By symmetry, we may assume that $2 \nmid B$. We proceed in four steps.

I. There exist k, e, $f \in \mathbb{N}$ such that

- $2 \nmid k$ and $k^2 q = e^2 - mf^2$;
- $(e,q) = (f,q) = (e,f) = (f,k) = (e,k) = (e,m) = (k,m) = 1$;
- $2 \mid f$ if $q \equiv m \equiv 1 \bmod 4$, and $2 \mid e$ if $-q \equiv m \equiv 1 \bmod 4$.

Proof of **I.** We prove first:

(*) If $k,\, e,\, f \in \mathbb{N}$ are such that $k^2q = e^2 - mf^2$ and $(k,e,f) = 1$, then it follows that $(e,q) = (f,q) = (e,f) = (f,k) = (e,k) = (e,m) = (k,m) = 1$.

Let $k,\, e,\, f \in \mathbb{N}$ be such that $k^2q = e^2 - mf^2$ and $(k,e,f) = 1$. If $q \,|\, e$ or $q \,|\, f$, then $q \,|\, (k,e,f)$, a contradiction. Hence $(e,q) = (f,q) = 1$.

Let now t be any prime and observe that m is squarefree. If $t \,|\, (e,f)$, then $t^2 \,|\, k^2q$, hence $t \,|\, k$ and thus $t \,|\, (k,e,f)$. If $t \,|\, (f,k)$, then $t \,|\, e$ and thus $t \,|\, (k,e,f)$. If $t \,|\, (e,k)$, then $t^2 \,|\, mf^2$, hence $t \,|\, f$ and thus $t \,|\, (k,e,f)$. If $t \,|\, (e,m)$ and $t \neq q$, then $t \,|\, k$ and thus $t \,|\, (k,e,f)$. If $t \,|\, (k,m)$, then $t \,|\, e$ and thus $t \,|\, (k,e,f)$. In each case, we arrive at the contradiction $t \,|\, (k,e,f)$. □[(*)]

Since m is a quadratic residue modulo q and $-q$ is a quadratic residue modulo m, Theorem 6.5.17 implies that there exists some triple $(k,e,f) \in \mathbb{Z}^3 \setminus \{(0,0,0)\}$ such that $k^2q - e^2 + mf^2 = 0$, and consequently $k^2q = e^2 - mf^2$. Since $q \nmid m$ and m is squarefree, it follows that $kef \neq 0$, and thus we may assume that $k,\, e,\, f \in \mathbb{N}$ and $(k,e,f) = 1$.

If $m \equiv 2 \mod 8$, then $e^2 - 2f^2 \equiv k^2q \mod 8$, and since $(e,f) = 1$, it follows that $2 \nmid k$, and we are done. If $m \equiv 1 \mod 4$, then we will eventually have to modify e, f and k in a suitable way. We distinguish two cases.

CASE a: $m \equiv q \equiv 1 \mod 4$. If $2 \,|\, f$, then $2 \nmid k$, and we are done. Thus suppose that $2 \nmid f$. Then $k^2 \equiv k^2q \equiv e^2 - mf^2 \equiv e^2 - 1 \mod 4$, and therefore $2 \,|\, k$. We set

$$k' = \Bigl|\frac{q-m}{2}\,k + mf\Bigr|, \quad e' = e\,\frac{q+m}{2}, \quad f' = \Bigl|\frac{q-m}{2}\,f - qk\Bigr|, \quad b = (e', f', k'),$$

$$k_1 = b^{-1}k', \quad e_1 = b^{-1}e' \quad \text{and} \quad f_1 = b^{-1}f'.$$

It follows that $k_1,\, e_1,\, f_1 \in \mathbb{N}$, $(k_1,e_1,f_1) = 1$, $k_1^2q = e_1^2 - mf_1^2$, $2 \nmid k_1$ and $2 \,|\, f_1$. Hence the triple (k_1,e_1,f_1) satisfies **I.**

CASE b: $m \equiv -q \equiv 1 \mod 4$. If $2 \,|\, e$, then $2 \nmid k$, and we are done. Thus suppose that $2 \nmid e$. Then $-k^2 \equiv k^2q \equiv e^2 - mf^2 \equiv 1 - f^2 \mod 4$, hence $2 \,|\, k$, and we consider the fundamental unit $\varepsilon_{4q} = u + v\sqrt{q} \in \mathcal{O}_{4q}^\times$, where $u,\, v \in \mathbb{N}$. Then $u^2 - qv^2 = 1$, Theorem 5.7.8.2 implies that $2 \,|\, u$, $2 \nmid v$, and we set

$$k' = ku + ev, \quad e' = eu + qkv, \quad b = (e', f, k'), \quad k_1 = b^{-1}k', \quad e_1 = b^{-1}e' \text{ and } f_1 = b^{-1}f.$$

It follows that $k_1,\, e_1,\, f_1 \in \mathbb{N}$, $(k_1,e_1,f_1) = 1$, $k_1^2q = e_1^2 - mf_1^2$, $2 \nmid k_1$ and $2 \,|\, e_1$. Hence the triple (k_1,e_1,f_1) satisfies **I.** □ [**I.**]

In the sequel we assume that $k,\, e,\, f \in \mathbb{N}$ are as in **I.** and observe that $2 \nmid aBk$.

II. $2 \nmid Af + Be$, and $(Af + Be,\, ae + Bf) = l^2$, where $l \in \mathbb{N}$ and $(l, 2ABqef) = 1$. If $t,\, u \in \mathbb{N}$ are such that $Af + Be = l^2t$ and $ae + Bf = l^2u$, then $(u,t) = 1$, $2 \nmid t$, and $t^2 - mu^2 = -qv^2$ for some $v \in \mathbb{N}$. Moreover,

$$\Bigl(\frac{Af + Be}{q}\Bigr) = (-1)^{\frac{t-1}{2}\,\frac{q-1}{2}} \Bigl(\frac{2}{tBk}\Bigr)^{\delta} \Bigl[\frac{q}{m_0}\Bigr]_4,$$

and if $u = 2^\theta u^*$, where $\theta \in \mathbb{N}_0$, $u^* \in \mathbb{N}$ and $2 \nmid u^*$, then

$$\Bigl(\frac{ae + Bf}{q}\Bigr) = (-1)^{\frac{u^*-1}{2}\,\frac{q+1}{2}}.$$

Proof of **II.** If $2\,|\,A$, then $2\nmid BC$, $m\equiv 2 \bmod 8$, $q\equiv k^2q\equiv e^2-2f^2 \bmod 8$, hence $2\nmid e$ and $Af+Be\equiv e\equiv 1 \bmod 2$. If $2\nmid A$, then $m\equiv 1 \bmod 4$, hence $2\,|\,e$ or $2\,|\,f$, and since $2\nmid B$, we obtain $Af+Be\equiv e+f\equiv 1 \bmod 2$.

Now we set $b=(Af+Be,ae+Bf)$, and we prove that every prime r dividing b satisfies $r\nmid 2ABqef$ and $2\,|\,\mathsf{v}_r(b)$. Thus let r be a prime such that $\mathsf{v}_r(b)=\kappa\geq 1$. Then $r\neq 2$, and from the identity

$$(Af+Be)^2-m(ae+Bf)^2=(B^2-ma^2)(e^2-mf^2)=-C^2k^2q$$

we obtain $r^{2\kappa}\,|\,C^2k^2q$. Since $q\nmid Ck$, it follows that

$$r\neq q\,,\quad r^\kappa\,|\,Ck\,,\quad \text{and if}\quad \lambda=\left\lceil\frac{\kappa}{2}\right\rceil,\quad \text{then}\quad r^\lambda\,|\,C\quad \text{or}\quad r^\lambda\,|\,k\,.$$

CASE a: $r^\lambda\,|\,k$. Then $r\nmid mef$, and since $r\,|\,ae+Bf$ and $(a,B)=1$, it follows that $r\nmid aB$. From $Af\equiv -Be \bmod r^\kappa$ and $ae\equiv -Bf \bmod r^\kappa$ we obtain

$$efma^2=(Af)(ae)\equiv(-Be)(-Bf)\equiv B^2ef \bmod r^\kappa,$$

hence $ma^2\equiv B^2 \bmod r^\kappa$, and therefore $r^\kappa\,|\,ma^2-B^2=C^2$, which implies $r^\lambda\,|\,C$.

CASE b: $r^\lambda\,|\,C$. Then $r\nmid aB$, and since $r\,|\,ae+Bf$ and $(e,f)=1$, it follows that $r\nmid ef$. From $Be\equiv -Af \bmod r^\kappa$ and $-Bf\equiv ae \bmod r^\kappa$ we obtain

$$Bak^2q=Ba(e^2-mf^2)=(Be)(ae)-(Bf)(Af)\equiv 0 \bmod r^\kappa,$$

hence $r^\kappa\,|\,k^2q$, and consequently $r^\lambda\,|\,k$.

In both cases, it follows that $r^\lambda\,|\,C$, $r^\lambda\,|\,k$, $r\nmid 2ABqef$, and $r\nmid m$, since $(m,C)=1$. We assume that κ is odd, say $\kappa=2\lambda-1$ for some $\lambda\in\mathbb{N}$. Since

$$m(a^2e^2-B^2f^2)=(ma^2-B^2)e^2+B^2(e^2-mf^2)=C^2e^2+B^2k^2q\equiv 0 \bmod r^{2\lambda}$$

and

$$A^2f^2-B^2e^2=mf^2(B^2+C^2)-B^2e^2=-B^2k^2q+mf^2C^2\equiv 0 \bmod r^{2\lambda}\,,$$

we obtain $r^{2\lambda}\,|\,(ae+Bf)(ae-Bf)$ and $r^{2\lambda}\,|\,(Af+Be)(Af-Be)$. Since $r\nmid 2ABef$, it follows that $r\nmid(ae+Bf,ae-Bf)$, $r\nmid(Af+Be,Af-Be)$, and therefore $r^{2\lambda}\,|\,ae+Bf$, $r^{2\lambda}\,|\,Af+Be$ and $r^{2\lambda}\,|\,b$. But then we get $\mathsf{v}_r(b)\geq 2\lambda=\kappa+1$, a contradiction.

Hence we have proved that $\kappa=\mathsf{v}_r(b)\equiv 0 \bmod 2$ and $\kappa\nmid 2ABqef$ for every prime r dividing b, and therefore $b=(Af+Be,ae+Bf)=l^2$ for some $l\in\mathbb{N}$ such that $(l,2ABqef)=1$.

We set $Af+Be=l^2t$ and $ae+Bf=l^2u$, where $u,\,t\in\mathbb{N}$, $(u,t)=1$, and $2\nmid t$ (since $2\nmid Af+Be$). As above, we obtain

$$l^4(t^2-mu^2)=(Af+Be)^2-m(ae+Bf)^2=-C^2k^2q\,,$$

hence $l^2\,|\,Ck$, and if $Ck=l^2v$, where $v\in\mathbb{N}$, then $t^2-mu^2=-qv^2$.

Now we calculate the following Jacobi symbols using the relations $k^2q=e^2-mf^2$ and $t^2-mu^2=-qv^2$. We obtain

$$\Big(\frac{Af+Be}{q}\Big)=\Big(\frac{l^2t}{q}\Big)=\Big(\frac{t}{q}\Big)=(-1)^{\frac{t-1}{2}\frac{q-1}{2}}\Big(\frac{q}{t}\Big),$$

$$\begin{aligned}\Big(\frac{q}{t}\Big) &= \Big(\frac{qv^2}{t}\Big) = \Big(\frac{mu^2}{t}\Big) = \Big(\frac{m}{t}\Big) = \Big(\frac{2}{t}\Big)^{\delta}\Big(\frac{m_0}{t}\Big) = \Big(\frac{2}{t}\Big)^{\delta}\Big(\frac{t}{m_0}\Big) = \Big(\frac{2}{t}\Big)^{\delta}\Big(\frac{l^2t}{m_0}\Big)\\ &= \Big(\frac{2}{t}\Big)^{\delta}\Big(\frac{Af+Be}{m_0}\Big) = \Big(\frac{2}{t}\Big)^{\delta}\Big(\frac{B}{m_0}\Big)\Big(\frac{e}{m_0}\Big) = \Big(\frac{2}{t}\Big)^{\delta}\Big(\frac{m_0}{B}\Big)\Big[\frac{e^2}{m_0}\Big]_4\\ &= \Big(\frac{2}{tB}\Big)^{\delta}\Big(\frac{m}{B}\Big)\Big[\frac{k^2q}{m_0}\Big]_4 = \Big(\frac{2}{tB}\Big)^{\delta}\Big(\frac{ma^2}{B}\Big)\Big(\frac{k}{m_0}\Big)\Big[\frac{q}{m_0}\Big]_4\\ &= \Big(\frac{2}{tB}\Big)^{\delta}\Big(\frac{B^2+C^2}{B}\Big)\Big(\frac{m_0}{k}\Big)\Big[\frac{q}{m_0}\Big]_4 = \Big(\frac{2}{tBk}\Big)^{\delta}\Big(\frac{m}{k}\Big)\Big[\frac{q}{m_0}\Big]_4 = \Big(\frac{2}{tBk}\Big)^{\delta}\Big[\frac{q}{m_0}\Big]_4,\end{aligned}$$

and therefore

$$\Big(\frac{Af+Be}{q}\Big) = (-1)^{\frac{t-1}{2}\frac{q-1}{2}}\Big(\frac{2}{tBk}\Big)^{\delta}\Big[\frac{q}{m_0}\Big]_4.$$

In the same way, it follows that

$$\Big(\frac{ae+Bf}{q}\Big) = \Big(\frac{l^2u}{q}\Big) = \Big(\frac{2}{q}\Big)^{\theta}\Big(\frac{u^*}{q}\Big) = (-1)^{\frac{u^*-1}{2}\frac{q-1}{2}}\Big(\frac{2}{q}\Big)^{\theta}\Big(\frac{q}{u^*}\Big),$$

$$\Big(\frac{q}{u^*}\Big) = \Big(\frac{qv^2}{u^*}\Big) = \Big(\frac{-t^2}{u^*}\Big) = (-1)^{\frac{u^*-1}{2}}, \quad \text{and} \quad \Big(\frac{ae+Bf}{q}\Big) = (-1)^{\frac{u^*-1}{2}\frac{q+1}{2}}\Big(\frac{2}{q}\Big)^{\theta}.$$

It remains to prove that either $2\nmid u$ (hence $\theta = 0$) or $q \equiv \pm 1 \bmod 8$. Assume to the contrary that $2\,|\,u$, and $q \equiv \pm 3 \bmod 8$. Since $2 \nmid tv$, it follows that

$$q \equiv qv^2 \equiv mu^2 - t^2 \equiv -1 \bmod 4\,, \quad \text{hence} \quad q \equiv 3 \bmod 8\,,$$

and $m \equiv mu^2 \equiv q+1 \equiv 4 \bmod 8$. By **I.** we have $2\,|\,f$, hence $2 \nmid e$, and since $l^2u = ae + Bf \equiv 0 \bmod 2$, we obtain $2\,|\,a$, a contradiction. $\square$ [**II.**]

III. Suppose that $e = 2^{\alpha}e^*$ and $f = 2^{\beta}f^*$, where $\alpha,\ \beta \in \mathbb{N}_0$, $e^*,\ f^* \in \mathbb{N}$, and $2 \nmid e^*f^*$. Then

$$\Big(\frac{e}{q}\Big) = (-1)^{\frac{e^*-1}{2}\frac{q+1}{2}}\Big(\frac{2}{qm_0}\Big)^{\alpha}\Big(\frac{2}{ke^*}\Big)^{\delta}\Big[\frac{q}{m_0}\Big]_4 \quad \text{and} \quad \Big(\frac{f}{q}\Big) = (-1)^{\frac{f^*-1}{2}\frac{q-1}{2}}\Big(\frac{2}{q}\Big)^{\beta}.$$

Proof of **III.** Calculating the Jacobi symbols as in **II.**, we obtain

$$\Big(\frac{e}{q}\Big) = \Big(\frac{2}{q}\Big)^{\alpha}\Big(\frac{e^*}{q}\Big) = (-1)^{\frac{e^*-1}{2}\frac{q-1}{2}}\Big(\frac{2}{q}\Big)^{\alpha}\Big(\frac{q}{e^*}\Big),$$

$$\begin{aligned}\Big(\frac{q}{e^*}\Big) &= \Big(\frac{k^2q}{e^*}\Big) = \Big(\frac{-mf^2}{e^*}\Big) = (-1)^{\frac{e^*-1}{2}}\Big(\frac{2}{e^*}\Big)^{\delta}\Big(\frac{m_0}{e^*}\Big) = (-1)^{\frac{e^*-1}{2}}\Big(\frac{2}{e^*}\Big)^{\delta}\Big(\frac{e^*}{m_0}\Big)\\ &= (-1)^{\frac{e^*-1}{2}}\Big(\frac{2}{e^*}\Big)^{\delta}\Big(\frac{2}{m_0}\Big)^{\alpha}\Big(\frac{e}{m_0}\Big) = (-1)^{\frac{e^*-1}{2}}\Big(\frac{2}{e^*}\Big)^{\delta}\Big(\frac{2}{m_0}\Big)^{\alpha}\Big[\frac{e^2}{m_0}\Big]_4\end{aligned}$$

and, since $e^2 \equiv k^2q \bmod m_0$ and $m \equiv e^2 \bmod k$,

$$\begin{aligned}\Big[\frac{e^2}{m_0}\Big]_4 &= \Big[\frac{k^2q}{m_0}\Big]_4 = \Big(\frac{k}{m_0}\Big)\Big[\frac{q}{m_0}\Big]_4 = \Big(\frac{m_0}{k}\Big)\Big[\frac{q}{m_0}\Big]_4 = \Big(\frac{2}{k}\Big)^{\delta}\Big(\frac{m}{k}\Big)\Big[\frac{q}{m_0}\Big]_4\\ &= \Big(\frac{2}{k}\Big)^{\delta}\Big[\frac{q}{m_0}\Big]_4.\end{aligned}$$

Putting all together, it follows that

$$\begin{aligned}\Big(\frac{e}{q}\Big) &= (-1)^{\frac{e^*-1}{2}\,\frac{q-1}{2}}\Big(\frac{2}{q}\Big)^{\alpha}(-1)^{\frac{e^*-1}{2}}\Big(\frac{2}{e^*}\Big)^{\delta}\Big(\frac{2}{m_0}\Big)^{\alpha}\Big(\frac{2}{k}\Big)^{\delta}\Big[\frac{q}{m_0}\Big]_4 \\ &= (-1)^{\frac{e^*-1}{2}\,\frac{q+1}{2}}\Big(\frac{2}{qm_0}\Big)^{\alpha}\Big(\frac{2}{ke^*}\Big)^{\delta}\Big[\frac{q}{m_0}\Big]_4 .\end{aligned}$$

Since $k^2q \equiv e^2 \mod f^*$, we obtain

$$\Big(\frac{f}{q}\Big) = \Big(\frac{2}{q}\Big)^{\beta}\Big(\frac{f^*}{q}\Big) = (-1)^{\frac{f^*-1}{2}\,\frac{q-1}{2}}\Big(\frac{2}{q}\Big)^{\beta}\Big(\frac{q}{f^*}\Big) = (-1)^{\frac{f^*-1}{2}\,\frac{q-1}{2}}\Big(\frac{2}{q}\Big)^{\beta}. \qquad \Box\,[\mathbf{III.}]$$

IV. Final proof. Throughout, we use **I.**, **II.** and **III.**

CASE 1: $q \equiv 1 \mod 4$, $q^* = q$. Since $mf^2 \equiv e^2 \mod q$, we obtain

$$\Big(\frac{f}{q}\Big)\Big(\frac{A+B\sqrt{m}}{q}\Big) = \Big(\frac{Af+B\sqrt{mf^2}}{q}\Big) = \Big(\frac{Af+Be}{q}\Big) = \Big(\frac{2}{tBk}\Big)^{\delta}\Big[\frac{q}{m_0}\Big]_4 ,$$

and therefore

$$\Big(\frac{A+B\sqrt{m}}{q}\Big) = \Big(\frac{f}{q}\Big)\Big(\frac{2}{tBk}\Big)^{\delta}\Big[\frac{q}{m_0}\Big]_4 = \Big(\frac{2}{q}\Big)^{\beta}\Big(\frac{2}{tBk}\Big)^{\delta}\Big[\frac{q}{m_0}\Big]_4 .$$

CASE 1a: $m \equiv 1 \mod 4$. Then $\delta = 0$, $m = m_0$ and $2\,|\,f$. We obtain

$$\Big(\frac{A+B\sqrt{m}}{q}\Big) = \Big(\frac{2}{q}\Big)^{\beta}\Big[\frac{q}{m}\Big]_4, \quad \text{and we must prove that} \quad \Big(\frac{2}{q}\Big)^{\beta} = \Big(\frac{2}{q}\Big).$$

This is obvious if $q \equiv 1 \mod 8$. If $q \equiv 5 \mod 8$, then $5 \equiv k^2q \equiv 1 - mf^2 \mod 8$, hence $f \equiv 2 \mod 4$ and $\beta = 1$.

CASE 1b: $m \equiv 2 \mod 8$. Then $\delta = 1$, $q \equiv 1 \mod 8$,

$$\Big(\frac{A+B\sqrt{m}}{q}\Big) = \Big(\frac{2}{tBk}\Big)\Big[\frac{q}{m_0}\Big]_4, \quad \text{and we must prove that} \quad (-1)^{(q-1)/8} = \Big(\frac{2}{tBk}\Big).$$

Since $1 \equiv k^2q \equiv e^2 - 2f^2 \mod 8$, it follows that $2 \nmid e$, $2\,|\,f$, $ABe \equiv A \equiv 2 \mod 4$, $Be(Af+Be) = ABef + B^2e^2 \equiv 2f+1 \mod 8$, and

$$\Big(\frac{2}{tBk}\Big) = \Big(\frac{2}{Bel^2t}\Big)\Big(\frac{2}{ke}\Big) = \Big(\frac{2}{Be(Af+Be)}\Big)\Big(\frac{2}{ke}\Big) = (-1)^{f/2+(k^2e^2-1)/8} .$$

Since $k^2e^2+4f-1 = k^4q + mf^2k^2 + 4f - 1 \equiv q - 1 + 2f(m_0f+2) \equiv q-1 \mod 16$, it follows that

$$\frac{f}{2} + \frac{k^2e^2-1}{8} \equiv \frac{q-1}{8} \mod 2 ,$$

which completes the proof.

CASE 2: $q \equiv 3 \mod 4$, $q^* = -q$. Since $me^2 \equiv m^2f^2 \mod q$, we obtain

$$\Big(\frac{e}{q}\Big)\Big(\frac{A+B\sqrt{m}}{q}\Big) = \Big(\frac{Ae+B\sqrt{me^2}}{q}\Big) = \Big(\frac{ame+Bmf}{q}\Big) = \Big(\frac{m}{q}\Big)\Big(\frac{ae+Bf}{q}\Big) = 1 ,$$

and therefore

$$\Big(\frac{A+B\sqrt{m}}{q}\Big) = \Big(\frac{e}{q}\Big) = \Big(\frac{2}{qm_0}\Big)^{\alpha}\Big(\frac{2}{ke^*}\Big)^{\delta}\Big[\frac{q}{m_0}\Big]_4 .$$

CASE 2a: $m \equiv 1 \bmod 4$. Then $\delta = 0$, $m_0 = m$, $qm \equiv 3 \bmod 4$, and

$$\Big(\frac{A+B\sqrt{m}}{q}\Big) = \Big(\frac{2}{qm}\Big)^{\alpha}\Big[\frac{-q^*}{m}\Big]_4 = \Big(\frac{2}{qm}\Big)^{\alpha}(-1)^{(m-1)/4}\Big[\frac{q^*}{m}\Big]_4 .$$

Hence we must prove that

$$\Big(\frac{2}{q\,m}\Big)^{\alpha}(-1)^{(m-1)/4} = \Big(\frac{2}{q}\Big),$$

which is equivalent to

$$\alpha\,\frac{q\,m+1}{4} + \frac{m-1}{4} \equiv \frac{q+1}{4} \bmod 2 \quad \text{or to} \quad \alpha(qm+1)+m-q \equiv 2 \bmod 8 .$$

If $q+m \equiv 0 \bmod 8$, then $qm+1 \equiv -m^2+1 \equiv 0 \bmod 8$, $m-q \equiv 2m \equiv 2 \bmod 8$, and we are done. Thus assume that $q+m \equiv 4 \bmod 8$. Then it follows that

$$qm \equiv m(4-m) \equiv 4m-1 \equiv 3 \mod 8 ,$$

and $3 \equiv k^2q \equiv e^2 - mf^2 \equiv e^2 - f^2 \bmod 4$, which implies $2 \,|\, e$ and $2 \nmid f$. Since $e^2 = k^2q + mf^2 \equiv q+m \equiv 4 \bmod 8$, we get $e \equiv 2 \bmod 4$, hence $\alpha = 1$, and again $\alpha(qm+1)+m-q \equiv 4+m-q \equiv 2m \equiv 2 \bmod 8$.

CASE 2b: $m \equiv 2 \bmod 8$. Then $\delta = 1$, $m = 2m_0$, $q \equiv 7 \bmod 8$, and therefore $7 \equiv k^2q \equiv e^2 - 2f^2 \bmod 8$. Hence $2 \nmid e$, $2 \nmid f$, $\alpha = 0$, and

$$\Big(\frac{A+B\sqrt{m}}{q}\Big) = \Big(\frac{2}{ke}\Big)\Big[\frac{q}{m_0}\Big]_4 = \Big(\frac{2}{ke}\Big)(-1)^{(m_0-1)/4}\Big[\frac{q^*}{m_0}\Big]_4 .$$

Therefore it remains to prove that

$$\Big(\frac{2}{ke}\Big)(-1)^{(m_0-1)/4} = (-1)^{(q+1)/8}, \quad \text{that is,} \quad \frac{k^2e^2-1}{8} + \frac{m_0-1}{4} \equiv \frac{q+1}{8} \mod 2 .$$

But $k^2e^2 - 1 + 2(m_0-1) \equiv k^4q + k^2mf^2 - 1 + m - 2 \equiv q + 2m - 3 \equiv q+1 \bmod 16$, and the assertion follows.

CASE **B.** $q \,|\, BC$. By symmetry, we may assume that $q \,|\, B$.

Since $2^{\delta}m_0a^2 = B^2 + C^2$ and $(B,C) = 1$, it follows by Theorem 3.4.1 that m_0a^2 is a product of primes $p \equiv 1 \bmod 4$, and since $B + \mathsf{i}C$ is $\mathbb{Z}[\mathsf{i}]$-primitive, it follows by unique factorization in $\mathbb{Z}[\mathsf{i}]$ that $B + C\mathsf{i} = (1+\mathsf{i})^{\delta}\eta\pi_1 \cdot \ldots \cdot \pi_r$, where $r \in \mathbb{N}$, $\eta \in D^{\times}$ and $\pi_1, \ldots, \pi_r \in D$ are primes such that $\pi_i \equiv 1 \bmod 2$ and $\pi_i D \neq \overline{\pi}_j D$ for all $i, j \in [1,r]$. Hence $m_0a^2 = p_1 \cdot \ldots \cdot p_r$, where $p_i = \mathcal{N}(\pi_i)$ for all $i \in [1,r]$, and after renumbering if necessary we may assume that $r = s + 2t$, where $s, t \in \mathbb{N}$, $m_0 = p_1 \cdot \ldots \cdot p_s$, $p_{s+j} = p_{s+2j}$ for all $j \in [1,t]$, and $a = p_{s+1} \cdot \ldots \cdot p_{s+t}$. We set $\mu = \pi_1 \cdot \ldots \cdot \pi_s$ and $\alpha = \pi_{s+1} \cdot \ldots \cdot \pi_{s+t}$. Then it follows that $B + C\mathsf{i} = (1+\mathsf{i})^{\delta}\eta\mu\alpha^2$, $a = \mathcal{N}(\alpha)$ and $m_0 = \mathcal{N}(\mu)$.

Since q^* is a quadratic residue modulo m_0, we obtain

$$\Big[\frac{q^*}{m_0}\Big]_4 = \Big(\frac{q^*}{\mu}\Big)_4 \in \{\pm 1\} \quad \text{and} \quad \Big(\frac{2^{\delta}m_0}{q}\Big) = \Big(\frac{2}{q}\Big)^{\delta}\Big(\frac{q^*}{m_0}\Big) = 1 .$$

Using Theorem 7.3.5.2, we get

$$\begin{aligned}\Big(\frac{A+B\sqrt{m}}{q}\Big) &= \Big(\frac{A}{q}\Big) = \Big(\frac{2^\delta m_0 a}{q}\Big) = \Big(\frac{a}{q}\Big) = \Big(\frac{q^*}{a}\Big) = \Big(\frac{q^*}{\alpha}\Big)_2 = \Big(\frac{q^*}{\mu}\Big)_4^2 \Big(\frac{q^*}{\alpha^2}\Big)_4 \\ &= \Big(\frac{q^*}{\mu}\Big)_4 \Big(\frac{q^*}{\mu\alpha^2}\Big)_4 = \Big[\frac{q^*}{m_0}\Big]_4 \Big(\frac{q^*}{\mu\alpha^2}\Big)_4 = \Big[\frac{q^*}{m_0}\Big]_4 \Big(\frac{\mu\alpha^2}{q}\Big)_4 .\end{aligned}$$

CASE **a.** $\delta = 0$. Then

$$\Big(\frac{\mu\alpha^2}{q}\Big)_4 = \Big(\frac{\eta^{-1}(B+\mathrm{i}C)}{q}\Big)_4 = \Big(\frac{\eta^{-1}\mathrm{i}}{q}\Big)_4 .$$

Since $B + C\mathrm{i} = \eta\mu\alpha^2 \equiv \eta \bmod 2$ and $B + C \equiv 1 \bmod 2$, we get $\eta \in \{\pm 1\}$ if $2 \nmid B$, $\eta \in \{\pm\mathrm{i}\}$ if $2 \,|\, B$, and in both cases it follows that

$$\Big(\frac{\eta^{-1}\mathrm{i}}{q}\Big)_4 = \Big(\frac{2}{q}\Big)^B$$

by Theorem 7.3.8.2.

CASE **b.** $\delta = 1$. Then $q \equiv \varepsilon \bmod 8$, and we obtain (using the Theorems 7.4.8 and 7.3.8.2)

$$\begin{aligned}\Big(\frac{\mu\alpha^2}{q}\Big)_4 &= \Big(\frac{1+\mathrm{i}}{q}\Big)_4 \Big(\frac{(1+\mathrm{i})\mu\alpha^2}{q}\Big)_4 = \mathrm{i}^{(q\varepsilon-1)/4} \Big(\frac{\eta^{-1}(B+\mathrm{i}C)}{q}\Big)_4 \\ &= (-1)^{(q\varepsilon-1)/8} \Big(\frac{\eta^{-1}\mathrm{i}}{q}\Big)_4 = (-1)^{(q-\varepsilon)/8} .\end{aligned}$$

□

Exercise 7.5.5. Let p and q be distinct odd primes, $p = a^2 + b^2$ and $q = c^2 + d^2$, where $a,\ b,\ c,\ d \in \mathbb{N}$, $2 \nmid ac$, and

$$\Big(\frac{p}{q}\Big) = \Big(\frac{q}{p}\Big) = 1 .$$

a) Show that Burde's reciprocity law

$$\Big[\frac{p}{q}\Big]_4 \Big[\frac{q}{p}\Big]_4 = \Big(\frac{ac-bd}{p}\Big)$$

is a special case of Theorem 7.5.4. Hint: Set $A = pq$, $B = b(c^2 - d^2) + 2acd$, $C = a(c^2 - d^2) - 2bcd$ and $m = p$.

b) Prove Fröhlich's reciprocity law (see [**30**]):

$$\Big[\frac{p}{q}\Big]_4 \Big[\frac{q}{p}\Big]_4 = \Big(\frac{a+b\mathrm{i}}{q}\Big) = \Big(\frac{c+d\mathrm{i}}{p}\Big) .$$

We continue with a generalization of the reciprocity law of Schönemann and Scholz. The original law, which connects biquadratic reciprocity with the quadratic character of fundamental units, is contained in Corollary 7.5.7 (compare [**94**] and [**93**]).

Theorem 7.5.6. *Assume that* $m = 2^\delta p_1 \cdot \ldots \cdot p_r > 1$, *where* $\delta \in \{0,1\}$ $r \in \mathbb{N}_0$, $p_1, \ldots, p_r$ *are distinct primes such that* $p_i \equiv 1 \bmod 4$ *for all* $i \in [1,r]$,

$$\Big(\frac{2}{q}\Big)^\delta = 1 \quad \textit{and} \quad \Big(\frac{p_i}{q}\Big) = 1 \quad \textit{for all} \ \ i \in [1,r]\,.$$

Suppose that $\alpha = T + U\sqrt{m}$, *where* $T,\, U \in \mathbb{N}$, $(mU, T) = 1$, *and* $\mathcal{N}(\alpha) = -C^2$ *for some* $C \in \mathbb{N}$,

1. *If* $\delta = 0$, *then* $m \equiv 1 \bmod 4$, *then*
$$\Big(\frac{\alpha}{q}\Big) = \Big(\frac{2}{q}\Big)^{C+1} \Big[\frac{m}{q}\Big]_4 \Big[\frac{q^*}{m}\Big]_4 .$$
2. *If* $\delta = 1$, *then* $m = 2m_0 \equiv 2 \bmod 8$, $q \equiv \varepsilon \bmod 8$ *for some* $\varepsilon \in \{\pm 1\}$, *and*
$$\Big(\frac{\alpha}{q}\Big) = (-1)^{(q-\varepsilon)/8} \Big[\frac{m}{q}\Big]_4 \Big[\frac{q^*}{m_0}\Big]_4 .$$

Proof. We set $A = mU$ and $B = T$. Then $T^2 - mU^2 = -C^2$, $A^2 = m(B^2 + C^2)$, and $(A,B) = (B,C) = (C,A) = 1$. Now Theorem 7.5.4 implies

$$\Big(\frac{mU + T\sqrt{m}}{q}\Big) = \Big(\frac{2}{q}\Big)^T \Big[\frac{q^*}{m}\Big]_4 \qquad \text{if} \quad m \equiv 1 \mod 4\,,$$

and

$$\Big(\frac{mU + T\sqrt{m}}{q}\Big) = (-1)^{(q-\varepsilon)/8} \Big[\frac{q^*}{m_0}\Big]_4 \qquad \text{if} \quad m \equiv 2 \mod 8\,.$$

Since m, $\mathcal{N}(\alpha)$ and $\mathcal{N}(\sqrt{m}\,) = -m$ are quadratic residues modulo q, we obtain

$$\Big(\frac{mU + T\sqrt{m}}{q}\Big) = \Big(\frac{\alpha\sqrt{m}}{q}\Big) = \Big(\frac{\alpha}{q}\Big)\Big(\frac{\sqrt{m}}{q}\Big) = \Big(\frac{\alpha}{q}\Big)\Big[\frac{m}{q}\Big]_4 .$$

If $m \equiv 1 \bmod 4$, then $T^2 + C^2 = mU^2$, and $(T,C) = 1$ implies $U \equiv 1 \bmod 2$, hence $T \equiv C + 1 \bmod 2$, and

$$\Big(\frac{\alpha}{q}\Big) = \Big(\frac{mU + T\sqrt{m}}{q}\Big)\Big[\frac{m}{q}\Big]_4 = \Big(\frac{2}{q}\Big)^{C+1} \Big[\frac{m}{q}\Big]_4 \Big[\frac{q^*}{m}\Big]_4 .$$

If $m \equiv 2 \bmod 8$, then

$$\Big(\frac{\alpha}{q}\Big) = \Big(\frac{mU + T\sqrt{m}}{q}\Big)\Big[\frac{m}{q}\Big]_4 = (-1)^{(q-\varepsilon)/8} \Big[\frac{m}{q}\Big]_4 \Big[\frac{q^*}{m_0}\Big]_4 . \qquad \square$$

Corollary 7.5.7 (Schönemann, Scholz)**.** *Let* p *and* q *be distinct primes satisfying* $p \equiv q \equiv 1 \bmod 4$. *Then*

$$\Big(\frac{p}{q}\Big) = 1 \quad \textit{implies} \quad \Big[\frac{p}{q}\Big]_4 \Big[\frac{q}{p}\Big]_4 = \Big(\frac{\varepsilon_q}{p}\Big) = \Big(\frac{\varepsilon_p}{q}\Big).$$

If $q \equiv 1 \bmod 8$ *and* $c,\, d \in \mathbb{N}$ *are such that* $q = c^2 + 2d^2$, *then*

$$\Big(\frac{\varepsilon_2}{q}\Big) = \Big(\frac{1 + \sqrt{2}}{q}\Big) = (-1)^{(q-1)/8} \Big[\frac{2}{q}\Big]_4 = (-1)^{d/2} .$$

Proof. By Theorem 5.2.3.1 we have $\varepsilon_p^3 \in \mathbb{Z}[\sqrt{p}]$, and Theorem 5.7.1 implies $\mathcal{N}(\varepsilon_p^3) = \mathcal{N}(\varepsilon_p) = -1$. Using Theorem 7.5.6 with $m = p$, $\alpha = \varepsilon_p^3$ and $C = 1$, we obtain

$$\Bigl(\frac{\varepsilon_p}{q}\Bigr) = \Bigl(\frac{\varepsilon_p^3}{q}\Bigr) = \Bigl[\frac{p}{q}\Bigr]_4 \Bigl[\frac{q}{p}\Bigr]_4 .$$

By symmetry, we may interchange p and q.

Assume now that $q = c^2 + 2d^2 \equiv 1 \bmod 8$. Then $2 \,|\, d$, and we apply Theorem 7.5.6 with $\alpha = \varepsilon_2 = 1 + \sqrt{2}$. By Theorem 7.5.1.2(b), we obtain

$$\Bigl(\frac{\varepsilon_2}{q}\Bigr) = (-1)^{(q-1)/8} \Bigl[\frac{2}{q}\Bigr]_4 = (-1)^{(q-1)/8+b/4} = (-1)^{d/2} . \qquad \square$$

Exercise 7.5.8. Suppose that $m = p_1 \cdot \ldots \cdot p_r$, where $r \in \mathbb{N}$ and $p_1, \ldots, p_r$ are distinct primes such that $p_i \not\equiv 3 \bmod 4$ for all $i \in [1, r]$. Let $q \equiv 1 \bmod 4$ be a prime such that

$$\Bigl(\frac{p_i}{q}\Bigr) = 1 \quad \text{for all} \quad i \in [1, r] ,$$

and assume that $\mathcal{N}(\varepsilon_m) = -1$. Prove that

$$\Bigl(\frac{\varepsilon_m}{q}\Bigr) = \prod_{i=1}^{m} \Bigl(\frac{\varepsilon_{p_i}}{q}\Bigr) \qquad \text{(see [\textbf{31}])}.$$

For primes m and n, the following result, essentially due to Dirichlet, is referred to as Lehmer's reciprocity law [**66**].

Theorem 7.5.9 (Dirichlet, Lehmer)**.** *Let* $m = a^2 + b^2$ *be odd and squarefree, where* $a, b \in \mathbb{N}$ *and* $2 \,|\, b$. *Let* $n \ge 2$ *be an odd integer,* $(n, m) = 1$, *and suppose that*

$$\Bigl(\frac{p}{q}\Bigr) = 1 \quad \textit{for all primes } p \textit{ dividing } m \textit{ and all primes } q \textit{ dividing } n.$$

Then m *is a quadratic residue modulo* n, $n^* = (-1)^{(n-1)/2}$ *is a quadratic residue modulo* m, *and*

$$\Bigl(\frac{m + b\sqrt{m}}{n}\Bigr) = \Bigl[\frac{n^*}{m}\Bigr]_4 .$$

In particular, if $n = q$ *is a prime, then*

$$\Bigl[\frac{q^*}{m}\Bigr]_4 = 1 \quad \textit{if} \quad q \,|\, b , \qquad \textit{and} \qquad \Bigl[\frac{q^*}{m}\Bigr]_4 = \Bigl(\frac{2}{q}\Bigr) \quad \textit{if} \quad q \,|\, a .$$

Proof. Suppose that $n = q_1 \cdot \ldots \cdot q_k$, where $k \in \mathbb{N}$ and $q_1, \ldots, q_k$ are odd primes. Then $n^* = q_1^* \cdot \ldots \cdot q_k^*$, where $q_i^* = (-1)^{(q_i-1)/2}$ for all $i \in [1, k]$. Since $p \equiv 1 \bmod 4$ for all primes p dividing m, it follows that

$$\Bigl(\frac{p}{q}\Bigr) = \Bigl(\frac{q}{p}\Bigr) = 1 \quad \text{for all primes } p \text{ dividing } m \text{ and all primes } q \text{ dividing } n.$$

Hence n^* is a quadratic residue modulo m, and m is a quadratic residue modulo n. Since $\mathcal{N}(m+b\sqrt{m}) = m^2 - b^2m = ma^2$, the quadratic symbol in question is defined, and we obtain

$$\Big(\frac{m+b\sqrt{m}}{n}\Big) = \prod_{i=1}^{k}\Big(\frac{m+b\sqrt{m}}{q_i}\Big) \quad \text{and} \quad \Big[\frac{n^*}{m}\Big]_4 = \prod_{i=1}^{k}\Big[\frac{q_i^*}{m}\Big]_4 .$$

Therefore it suffices to prove the theorem when $n = q$ is an odd prime.

Since m is squarefree, we obtain $(a,b) = (a,m) = (b,m) = 1$, and Theorem 7.5.4, applied with $A = m$, $B = b$ and $C = a$, shows that

$$\Big(\frac{m+b\sqrt{m}}{q}\Big) = \Big[\frac{q^*}{m}\Big]_4 , \quad \text{and therefore} \quad \Big[\frac{q^*}{m}\Big]_4 = \Big(\frac{m}{q}\Big) = 1 \ \text{ if } \ q \,|\, b\,.$$

If $q \,|\, a$, then $m \equiv b^2 \bmod q$, and

$$\Big[\frac{q^*}{m}\Big]_4 = \Big(\frac{m+b\sqrt{m}}{q}\Big) = \Big(\frac{m+b^2}{q}\Big) = \Big(\frac{2b^2}{q}\Big) = \Big(\frac{2}{q}\Big)\,. \qquad \square$$

Immediately from Lehmer's reciprocity law, we obtain the following criteria for biquadratic residues which are due to Dirichlet.

Theorem 7.5.10 (Criteria for biquadratic residues 1)**.** *Let p and q be distinct odd primes, $p = a^2+b^2$, where $a,\ b \in \mathbb{N}$, $2 \,|\, b$, and let q be a quadratic residue modulo p. Then q^* is a biquadratic residue modulo p if and only if one of the following conditions is satisfied*:

- $q \,|\, b\,;$
- $q \,|\, a$ *and* $q \equiv \pm 1 \bmod 8\,;$
- $q \nmid ab$, *and there exist* $\lambda,\ \mu \in [1, q-1]$ *such that*

$$a \equiv \mu b \bmod q\,, \quad \mu^2 + 1 \equiv \lambda^2 \bmod q \quad \textit{and} \quad \Big(\frac{\lambda(\lambda+1)}{q}\Big) = 1\,.$$

PROOF. By Theorem 7.5.9,

$$\Big[\frac{q^*}{p}\Big]_4 = 1 \quad \text{if} \quad q \,|\, b\,, \quad \text{and} \quad \Big[\frac{q^*}{p}\Big]_4 = \Big(\frac{2}{q}\Big) \quad \text{if} \quad q \,|\, a\,.$$

Thus we may assume that $q \nmid ab$. Then there exists a unique $\mu \in [1, q-1]$ such that $a \equiv \mu b \bmod q$, and we obtain

$$1 = \Big(\frac{q}{p}\Big) = \Big(\frac{p}{q}\Big) = \Big(\frac{\mu^2b^2 + b^2}{q}\Big) = \Big(\frac{\mu^2+1}{q}\Big)\,.$$

If $\lambda \in [1, q-1]$ is such that $\lambda^2 \equiv 1 + \mu^2 \bmod q$, then $p = a^2 + b^2 \equiv b^2\lambda^2 \bmod q$, and by Theorem 7.5.9 we obtain

$$\Big[\frac{q^*}{p}\Big]_4 = \Big(\frac{p+b\sqrt{p}}{q}\Big) = \Big(\frac{p+b^2\lambda}{q}\Big) = \Big(\frac{b^2\lambda^2 + b^2\lambda}{q}\Big) = \Big(\frac{\lambda(\lambda+1)}{q}\Big)\,. \qquad \square$$

Examples 7.5.11. Let $p = a^2 + b^2$ be a prime, where $a,\ b \in \mathbb{N}$ and $2 \,|\, b$. Then

- -3 is a biquadratic residue modulo p if and only if $3 \,|\, b\,;$
- 5 is a biquadratic residue modulo p if and only if $5 \,|\, b\,;$

- -7 is a biquadratic residue modulo p if and only if $7 \,|\, ab$;
- -11 is a biquadratic residue modulo p if and only if
$$\text{either} \;\; 11 \,|\, b \;\; \text{or} \;\; a \equiv \pm 2b \mod 11\,;$$
- 13 is a biquadratic residue modulo p if and only if
$$\text{either} \;\; 13 \,|\, b \;\; \text{or} \;\; a \equiv \pm 3b \mod 13\,;$$

We give details for $q = 7$ and $q = 13$.

$q = 7$: If $7 \,|\, ab$, then $7 \,|\, a$ or $7 \,|\, b$, and in both cases -7 is a biquadratic residue modulo p by Theorem 7.5.10. Thus assume that $7 \nmid ab$. Then it suffices to prove that there are no $\lambda,\ \mu \in [1,6]$ such that $\lambda^2 \equiv 1+\mu^2 \mod 7$ and $\lambda(\lambda+1)$ is a quadratic residue modulo 7.

Indeed, if $\mu \in [1,6]$, then $\mu^2 + 1 \equiv 2,\ 3$ or $5 \mod 7$, and if $\lambda^2 \equiv 1 + \mu^2 \mod 7$, then $\lambda \equiv \pm 3 \mod 7$, and consequently $\lambda(\lambda+1) \equiv 5$ or $6 \mod 7$. But 5 and 6 are not quadratic residues modulo 7.

$q = 13$: If $13 \,|\, b$, then 13 is a biquadratic residue modulo p, and if $13 \,|\, a$, then 13 is not a biquadratic residue modulo p (by Theorem 7.5.10). Note that

$$\{1,\ 3,\ 4,\ 9,\ 10,\ 12\} = \bigl\{c \in [1,12] \bigm| c \text{ is a quadratic residue modulo } 13\bigr\}\,.$$

If $\lambda,\ \mu \in [1,12]$ are such that $\lambda^2 \equiv \mu^2 + 1 \mod 13$, then $\lambda^2 \equiv 4$ or $10 \mod 13$, and thus $\lambda \equiv \pm 2$ or $\pm 6 \mod 13$. If $\lambda \equiv \pm 2 \mod 13$, then $\lambda(\lambda+1) \equiv 6$ or $2 \mod 13$, and if $\lambda \equiv \pm 6 \mod 13$, then $\lambda(\lambda+1) \equiv 3$ or $4 \mod 13$. Since $\lambda \equiv \pm 6 \mod 13$ implies $\mu \equiv \pm 3 \mod 13$, the assertion follows.

We close this section with a further biquadratic reciprocity law, due to E. Lehmer [**66**] and E. Brown [**11**], which connects biquadratic reciprocity with class numbers and once more with the quadratic character of quadratic units.

Theorem 7.5.12 (Lehmer, Brown)**.** *Let p and q be distinct odd primes such that $p \equiv q \equiv 1 \mod 4$ and*

$$\Bigl(\frac{p}{q}\Bigr) = 1\,.$$

1. *If $s^2 p = c^2 + qd^2$ for some odd $s \in \mathbb{N}$ such that $(s,q) = 1$, then*
$$\Bigl(\frac{\varepsilon_q}{p}\Bigr) = \Bigl(\frac{2}{q}\Bigr)^d \Bigl(\frac{s}{q}\Bigr)\,.$$
2. *Suppose that $q \equiv 5 \mod 8$. Then $h_{-4q} \equiv 2 \mod 4$, there exist $c,\ d,\ l \in \mathbb{N}$ such that $2 \nmid l$ and $p^l = c^2 + qd^2$. Whenever positive integers $c,\ d,\ l$ have these properties, then*
$$\Bigl[\frac{p}{q}\Bigr]_4 \Bigl[\frac{q}{p}\Bigr]_4 = (-1)^d\,.$$

PROOF. 1. From

$$\Big[\frac{q}{p}\Big]_4\Big(\frac{d}{p}\Big)=\Big[\frac{qd^2}{p}\Big]_4=\Big[\frac{-c^2}{p}\Big]_4=\Big[\frac{-1}{p}\Big]_4\Big(\frac{c}{p}\Big)=\Big(\frac{2c}{p}\Big)\quad\text{we get}\quad\Big[\frac{q}{p}\Big]_4=\Big(\frac{2cd}{p}\Big),$$

and from

$$\Big(\frac{s}{q}\Big)\Big[\frac{p}{q}\Big]_4=\Big[\frac{s^2p}{q}\Big]_4=\Big[\frac{c^2}{q}\Big]_4=\Big(\frac{c}{q}\Big)\quad\text{we get}\quad\Big[\frac{p}{q}\Big]_4=\Big(\frac{sc}{q}\Big).$$

Now we apply Corollary 7.5.7 and obtain

$$\Big(\frac{\varepsilon_q}{p}\Big)=\Big(\frac{2cd}{p}\Big)\Big(\frac{sc}{q}\Big).$$

CASE 1: $c\equiv 1 \bmod 2$. Then $2\,|\,d$, and we set $d=2^\delta d^*$, where δ, $d^*\in\mathbb{N}$ and $2\nmid d^*$. Since $p\equiv 1+qd^2 \bmod 8$, it follows that $p\equiv 1 \bmod 8$ if $\delta\geq 2$, and we obtain

$$\Big(\frac{2d}{p}\Big)=\Big(\frac{2^{\delta+1}d^*}{p}\Big)=\Big(\frac{d^*}{p}\Big)=\Big(\frac{p}{d^*}\Big)=\Big(\frac{s^2p}{d^*}\Big)=1\,.$$

Moreover,

$$\Big(\frac{c}{q}\Big)=\Big(\frac{q}{c}\Big)=\Big(\frac{qd^2}{c}\Big)=\Big(\frac{s^2p}{c}\Big)=\Big(\frac{p}{c}\Big)=\Big(\frac{c}{p}\Big),$$

and therefore

$$\Big(\frac{\varepsilon_q}{p}\Big)=\Big(\frac{2cd}{p}\Big)\Big(\frac{sc}{q}\Big)=\Big(\frac{2d}{p}\Big)\Big(\frac{c}{p}\Big)\Big(\frac{c}{q}\Big)\Big(\frac{s}{q}\Big)=\Big(\frac{s}{q}\Big).$$

CASE 2: $c\equiv 0 \bmod 2$. Then $2\nmid d$, and we set $c=2^\gamma c^*$, where γ, $c^*\in\mathbb{N}$ and $2\nmid c^*$. Since $s^2pq=d^2q+q^2d^2$, it follows that $pq\equiv 1 \bmod 8$ if $\gamma\geq 2$, and we obtain

$$\Big(\frac{2c}{pq}\Big)=\Big(\frac{2}{pq}\Big)^{\gamma+1}\Big(\frac{c^*}{pq}\Big)=\Big(\frac{c^*}{pq}\Big)=\Big(\frac{pq}{c^*}\Big)=\Big(\frac{s^2pq}{c^*}\Big)=1\,.$$

Moreover,

$$\Big(\frac{d}{p}\Big)=\Big(\frac{p}{d}\Big)=\Big(\frac{s^2p}{d}\Big),$$

and therefore

$$\Big(\frac{\varepsilon_q}{p}\Big)=\Big(\frac{2cd}{p}\Big)\Big(\frac{sc}{q}\Big)=\Big(\frac{2c}{pq}\Big)\Big(\frac{2s}{q}\Big)\Big(\frac{d}{q}\Big)=\Big(\frac{2}{q}\Big)\Big(\frac{s}{q}\Big).$$

2. We use genus theory for the fundamental discriminant $\Delta=-4q$. There are two basic genus characters ε and χ associated with this discriminant, given by

$$\varepsilon(C)=(-1)^{(m-1)/2}\quad\text{if } m\in\mathbb{Z}\setminus 2\mathbb{Z},\quad\text{and}\quad C\text{ represents } m,$$

and

$$\chi(C)=\Big(\frac{m}{p}\Big)\quad\text{if } m\in\mathbb{Z}\setminus p\mathbb{Z},\quad\text{and}\quad C\text{ represents } m.$$

The class $F=[\![2,2,(p+1)/2]\!]\in\mathfrak{F}_\Delta$ is ambiguous, and as

$$\chi(F)=\Big(\frac{2}{q}\Big)=-1\,,$$

F is not a square. Since $|\mathfrak{F}_\Delta/\mathfrak{F}_\Delta^2|=2^{\mu(\Delta)-1}=2$, it follows that $|\mathfrak{F}_\Delta|=2l$ for some odd $l\in\mathbb{N}$. Since $-4q$ is a quadratic residue modulo p, it follows that p is represented by some class $C \in \mathfrak{F}_\Delta$, and (by definition) $\varepsilon(C) = \chi(C) = 1$. Hence it follows that $C \in \mathfrak{F}_\Delta^2$ and $C^l = H_\Delta = [\![1, 0, q]\!]$. Therefore H_Δ represents p^l, and there exist $c,\ d \in \mathbb{N}$ such that $p^l = c^2 + qd^2$.

For any positive integers $c,\ d,\ l$ such that $2 \nmid l$ and $p^l = c^2 + qd^2$, we apply 1. with $s = p^{(l-1)/2}$ and obtain (with the aid of Corollary 7.5.7)

$$\Big[\frac{p}{q}\Big]_4 \Big[\frac{q}{p}\Big]_4 = \Big(\frac{\varepsilon_q}{p}\Big) = \Big(\frac{2}{q}\Big)^d \Big(\frac{p^{(l-1)/2}}{q}\Big) = (-1)^d . \qquad \Box$$

7.6. A biquadratic class group character and applications

The results of this section are based on the work of Z.-H. Sun [**101**], [**102**]. We use biquadratic Jacobi symbols to construct certain class group characters $\chi\colon \mathfrak{F}_\Delta \to \mathbb{C}^\times$ of order 4 in an explicit way. We confess that this construction is highly non-transparent. The result however, is clear, and it yields explicit criteria for biquadratic residues of rational numbers (Theorem 7.6.4 and Example 7.6.5) and quadratic residues of certain quadratic units (Corollary 7.6.7 and Example 7.6.8). Although existence and uniqueness of these characters follow from class field theory, the general theory gives no hint for an explicit construction.

We start with a highly technical result concerning the values of relevant biquadratic Jacobi symbols. Only in the following Theorem 7.6.2 does the usefulness of these calculations become understandable.

Theorem 7.6.1. *Let* $a,\ b,\ c,\ d,\ k,\ u,\ v,\ x,\ y \in \mathbb{Z}$ *be such that* $2 \,|\, kd$, $(u, v) = 1$, $b^2 - ac = -k^2 d$, $dv(u^2 - dv^2) \ne 0$, $\big(a(ax^2 + 2bxy + cy^2),\, 2ky(u^2 - dv^2)\big) = 1$, *and set* $u^2 - dv^2 = (-1)^r 2^s W$, *where* $r \in \{0, 1\}$, $s \in \mathbb{N}_0$, $W \in \mathbb{Z}$ *and* $W \equiv 1 \bmod 4$. *Let w be the product of all primes dividing W, and suppose that* $w \,|\, ku$.

1. *Suppose that*

$$2 \,\Big|\, \frac{ku}{(k, v)}, \quad 4 \,\Big|\, \frac{ksu}{(k, v)} \quad \text{and} \quad S = \frac{ku}{2(k, v)} \Big[\frac{s}{2} + r + 1 + \frac{k^2 d}{2} + \mathsf{v}_2\Big(\frac{k}{v}\Big) \Big].$$

Then $((ax + by)v + kuy\mathsf{i}, ax^2 + 2bxy + cy^2) = (bv - ku\mathsf{i}, a) = 1$, $S \in \mathbb{Z}$, *and*

$$\Big(\frac{(ax + by)v + kuy\mathsf{i}}{ax^2 + 2bxy + cy^2}\Big)_4 = (-1)^{Sy} \Big(\frac{bv - ku\mathsf{i}}{a}\Big)_4 .$$

2. *Assume that the following conditions are fulfilled*:
   - (a) *If* $2 \nmid s$, *then* $\mathsf{v}_2(k) \ge \mathsf{v}_2(v) + \max\{3 - \mathsf{v}_2(u),\, 0\}$.
   - (b) *If* $2 \,|\, s$ *and* $2 \nmid u$, *then* $\mathsf{v}_2(k) \ge 1 + \mathsf{v}_2(v)$.
   - (c) *If* $2 \,|\, s$, $2 \nmid u$ *and* $4 \nmid 2r + s$, *then* $\mathsf{v}_2(k) \ge 2 + \mathsf{v}_2(v)$.
   - (d) *If* $2 \,|\, s$, $u \equiv 2 \bmod 4$ *and* $d + 2r + s \not\equiv 2 \bmod 4$, *then* $2 \,|\, k$.

Then $((ax + by)v + kuy\mathsf{i}, ax^2 + 2bxy + cy^2) = (bv - ku\mathsf{i}, a) = 1$, *and*

$$\Big(\frac{(ax + by)v + kuy\mathsf{i}}{ax^2 + 2bxy + cy^2}\Big)_4 = \Big(\frac{bv - ku\mathsf{i}}{a}\Big)_4 .$$

Proof. We freely use the properties of quadratic and biquadratic Jacobi symbols.

1. Observe that

$$S = \frac{kus}{4(k,v)} + \frac{k^2d}{2}\,\frac{ku}{2(k,v} + \frac{ku}{2(k,v)}\,[\,r+1+\mathsf{v}_2(k)-\mathsf{v}_2(v)] \in \mathbb{Z}\,.$$

First we assert:

A. $(v,ky) = (k,v)\Big(\dfrac{v}{(k,v)}, y\Big)$, and $2 \nmid (ax+by)\dfrac{v}{(k,v)}$.

Proof of **A.** Obviously,

$$(k,v)\Big(\frac{v}{(k,v)}, y\Big) = \big(v, (k,v)y\big) = (v, ky, vy) = (v,ky)\,.$$

If $2 \,|\, ax+by$, then $2 \,|\, (ax+by)^2 + k^2dy^2 = a(ax^2+2bxy+cy^2)$, and if

$$2 \,\Big|\, \frac{v}{(k,v)}\,, \quad \text{then} \quad 2 \,\Big|\, \Big(\frac{ku}{(k,v)}, \frac{v}{(k,v)}\Big) \,\Big|\, u\,, \quad \text{hence} \quad 2 \,|\, (u,v)\,.$$

Thus in both cases we arrive at a contradiction. □[**A.**]

Now we set

$$v_0 = \frac{v}{(v,ky)}\,, \quad A = (ax+by)v_0\,, \quad k_0 = \frac{ky}{(v,ky)} \quad \text{and} \quad B = k_0u\,.$$

Then it follows that $(v_0,k_0)=1$, $kyv_0 = k_0v$, $(ax+by)v + kuy\mathsf{i} = (A+B\mathsf{i})(v,ky)$, and we assert:

B. $(A+B\mathsf{i},\, a(ax^2+2bxy+cy^2)v_0) = 1$, $2 \nmid A$, $2 \,|\, B$, and

$$B \equiv By \equiv \frac{kuy}{(k,v)} \mod 4\,.$$

Proof of **B.** Assume to the contrary that $(A+B\mathsf{i},\, a(ax^2+2bxy+cy^2)v_0) \ne 1$. Then there is some prime t such that $t \,|\, A^2+B^2$ and $t \,|\, a(ax^2+2bxy+cy^2)v_0$. Since

$$a(ax^2+2bxy+cy^2)v_0^2 = \big[(ax+by)v_0\big]^2 + k^2dy^2v_0^2 = A^2+B^2-(u^2-dv^2)k_0^2\,,$$

it follows that $t \,|\, (u^2-dv^2)k_0 \,|\, ky(u^2-dv^2)$, hence $t \nmid a(ax^2+2bxy+cy^2)$, and therefore $t \,|\, v_0 \,|\, v$. Since $(v_0,k_0)=1$, we obtain $t \nmid k_0$, hence $t \,|\, u^2-dv^2$ and $t \,|\, (u,v)$, a contradiction. Since

$$A = (ax+by)\frac{v}{(v,ky)} \,\Big|\, (ax+by)\frac{v}{(k,v)}\,, \quad \textbf{A} \text{ implies} \quad 2 \nmid A\,.$$

By assumption and, again using **A**, we have

$$2 \,\Big|\, \frac{ku}{(k,v)}\,, \quad 2 \nmid \Big(\frac{v}{(k,v)}, y\Big) \quad \text{and} \quad B = \frac{kuy}{(v,ky)} = \frac{ku}{(k,v)}\,\frac{y}{\big(\frac{v}{(k,v)}, y\big)} \equiv \frac{kuy}{(k,v)} \mod 4\,.$$

In particular, $2 \,|\, B$, and therefore

$$By = \frac{kuy^2}{(k,v)} \equiv \frac{kuy}{(k,v)} \equiv B \mod 4\,.$$

□[**B**.]

Since $(ax+by)v+kuy\mathsf{i}=(A+B\mathsf{i})(v,ky)$, $(A+B\mathsf{i},\,a(ax^2+2bxy+cy^2)v_0)=1$ and $((v,ky),\,ax^2+2bxy+cy^2)=1$, we obtain

$$\begin{aligned}J&=\Big(\frac{(ax+by)v+kuy\mathsf{i}}{ax^2+2bxy+cy^2}\Big)_4=\Big(\frac{A+B\mathsf{i}}{ax^2+2bxy+cy^2}\Big)_4\Big(\frac{(v,ky)}{ax^2+2bxy+cy^2}\Big)_4\\&=\Big(\frac{A+B\mathsf{i}}{ax^2+2bxy+cy^2}\Big)_4=\Big(\frac{A+B\mathsf{i}}{a(ax^2+2bxy+cy^2)v_0^2}\Big)_4\Big(\frac{A+B\mathsf{i}}{av_0^2}\Big)_4^{-1}\\&=\Big(\frac{\varepsilon}{A+B\mathsf{i}}\Big)_4\Big(\frac{a(ax^2+2bxy+cy^2)v_0^2}{A+B\mathsf{i}}\Big)_4\Big(\frac{A-B\mathsf{i}}{a}\Big)_4\Big(\frac{A-B\mathsf{i}}{v_0}\Big)_4^2,\end{aligned}$$

where $\varepsilon\in\{\pm1\}$ is such that $\varepsilon\equiv a(ax^2+2bxy+cy^2)v_0^2 \bmod 4$.

Since $2\nmid(ax+by)v_0$ by **A** and $2\,|\,kd$, it follows that $k^2dy^2\equiv k^2dy \bmod 4$,

$$a(ax^2+2bxy+cy^2)v_0^2=[(ax+by)^2+k^2dy^2]v_0^2\equiv 1+k^2dy\equiv(-1)^{k^2dy/2} \mod 4\,,$$

and therefore $\varepsilon=(-1)^{k^2dy/2}$. Since

$$a(ax^2+2bxy+cy^2)v_0^2=A^2+B^2-(u^2-dv^2)k_0^2\equiv-(u^2-dv^2)k_0^2 \mod A+B\mathsf{i}$$

and $u^2-dv^2=(-1)^r2^sW$, we get

$$J=\Big(\frac{-1}{A+B\mathsf{i}}\Big)_4^{k^2dy/2+r+1}\Big(\frac{2^sWk_0^2}{A+B\mathsf{i}}\Big)_4\Big(\frac{A-B\mathsf{i}}{a}\Big)_4\Big(\frac{A-B\mathsf{i}}{v_0}\Big)_4^2.$$

Now we obtain

$$\Big(\frac{-1}{A+B\mathsf{i}}\Big)_4=(-1)^{B/2}\,,\quad \Big(\frac{A-B\mathsf{i}}{v_0}\Big)_4^2=\Big(\frac{-B\mathsf{i}}{v_0}\Big)_4^2=\Big(\frac{-B_0^2}{v_0}\Big)_4=1\,,$$

$(A-B\mathsf{i})(v,ky)=(ax+by)v-uky\mathsf{i}\equiv(bv-uk\mathsf{i})y \bmod a$, $(a,(v,ky))=1$, and therefore

$$\Big(\frac{A-B\mathsf{i}}{a}\Big)_4=\Big(\frac{(A-B\mathsf{i})(v,ky)}{a}\Big)_4=\Big(\frac{(bv-ku\mathsf{i})y}{a}\Big)_4=\Big(\frac{bv-ku\mathsf{i}}{a}\Big)_4.$$

Putting all together, we find

$$J=(-1)^{(k^2dy/2+r+1)B/2}\Big(\frac{2^sWk_0^2}{A+B\mathsf{i}}\Big)_4\Big(\frac{bv-ku\mathsf{i}}{a}\Big)_4.$$

We set $t=\mathsf{v}_2(y)$, hence $2\,|\,ty$, and

$$n=\mathsf{v}_2\Big(\frac{k}{(k,v)}\Big)=\mathsf{v}_2(k)-\mathsf{v}_2(v)+\mathsf{v}_2\Big(\frac{v}{(k,v)}\Big)=\mathsf{v}_2\Big(\frac{k}{v}\Big)\quad\text{by }\mathbf{A.}$$

Using **A** once more, we get

$$k_0=\frac{ky}{(v,ky)}=\frac{k}{(k,v)}\,\frac{y}{\big(\frac{v}{(k,v)},y\big)}\quad\text{and}\quad\mathsf{v}_2\Big(\frac{v}{(k,v)}\Big)=0\,,$$

hence $\mathsf{v}_2(k_0)=n+t$, and we set $k_0=2^{n+t}M$, where $M\in\mathbb{Z}$ and $2\nmid M$. By **B** we obtain $k^2dyB\equiv k^2dB \bmod 8$, and therefore

$$\begin{aligned}J&=(-1)^{(k^2dy/2+r+1)B/2}\Big(\frac{2}{A+B\mathsf{i}}\Big)_4^{s+2n+2t}\Big(\frac{M^2W}{A+B\mathsf{i}}\Big)_4\Big(\frac{bv-ku\mathsf{i}}{a}\Big)_4\\&=\mathsf{i}^{(k^2d/2+r+1)B-(s+2n+2t)(A+B)B/2}\Big(\frac{M^2W}{A+B\mathsf{i}}\Big)_4\Big(\frac{bv-ku\mathsf{i}}{a}\Big)_4.\end{aligned}$$

Since $M^2W \equiv 1 \bmod 4$ and $M \,|\, B$, we get

$$\Big(\frac{M^2W}{A+B\mathsf{i}}\Big)_4 = \Big(\frac{A+B\mathsf{i}}{M^2W}\Big)_4 = \Big(\frac{A+B\mathsf{i}}{M}\Big)_4^2\Big(\frac{A+B\mathsf{i}}{W}\Big)_4 = \Big(\frac{A}{M}\Big)_4^2\Big(\frac{A+B\mathsf{i}}{W}\Big)_4$$
$$= \Big(\frac{A+B\mathsf{i}}{W}\Big)_4 = \prod_{\substack{p\in\mathbb{P}\\ p\,|\,W}}\Big(\frac{A+B\mathsf{i}}{p}\Big)_4^{\mathsf{v}_p(W)}.$$

Let p be a prime such that $p \,|\, W$. Then $u^2 = dv^2 + (-1)^r 2^s W \equiv dv^2 \bmod p$, since $(u,v)=1$ we obtain $p \nmid v$, and since $p \,|\, w \,|\, ku$, it follows that

$$p \,\Big|\, \frac{ku}{(k,v)} \,\Big|\, \frac{kuy}{(v,ky)} = B\,, \quad \text{and} \quad \Big(\frac{A+B\mathsf{i}}{p}\Big)_4 = \Big(\frac{A}{p}\Big)_4 = 1\,.$$

Hence

$$\Big(\frac{M^2W}{A+B\mathsf{i}}\Big)_4 = 1\,,$$

and we must prove that

$$\Big(r+1+\frac{k^2d}{2}\Big)B - (s+2n+2t)\,\frac{(A+B)B}{2} \equiv 2Sy \bmod 4\,.$$

Since

$$\Big(\frac{v}{(k,v)},y\Big)^2 \equiv 1 \bmod 4 \quad \text{and} \quad \Big(\frac{kuy}{2(k,v)}\Big)^2 \equiv \frac{kuy}{2(k,v)} \bmod 2\,,$$

we obtain

$$\frac{(A+B)B}{2} = \frac{kuy[(ax+by)v+kuy]}{2(k,v)^2\big(\frac{v}{(k,v)},y\big)^2} \equiv \frac{kuy[(ax+by)v+kuy]}{2(k,v)^2}$$
$$\equiv \frac{kuvy(ax+by)}{2(k,v)^2} + 2\Big(\frac{kuy}{2(k,v)}\Big)^2 \equiv \frac{kuy}{2(k,v)}\Big[(ax+by)\frac{v}{(k,v)}+2\Big] \bmod 4\,.$$

Now we observe that

$$2 \,|\, ty\,, \quad \frac{kus}{2(k,v)} \equiv 0 \bmod 2 \quad \text{and} \quad (ax+by)\frac{v}{(k,v)} \equiv 1 \bmod 2\,,$$

and thus we find

$$-(s+2n+2t)\frac{(A+B)B}{2} \equiv -s\frac{kuy}{2(k,v)}\Big[(ax+by)\frac{v}{(k,v)}+2\Big] + 2n\frac{kuy}{2(k,v)}$$
$$\equiv \frac{kuy}{2(k,v)}\Big[2s+2n-s(ax+by)\frac{v}{(k,v)}\Big] \equiv \frac{kuy}{2(k,v)}(2n+s) \bmod 4\,.$$

Putting all together, we obtain

$$\Big(r{+}1+\frac{k^2d}{2}\Big)B - (s+2n+2t)\frac{(A+B)B}{2} \equiv \frac{kuy}{(k,v)}\Big(r{+}1+\frac{k^2d}{2}\Big) + \frac{kuy}{2(k,v)}(2n+s)$$
$$\equiv 2y\,\frac{ku}{2(k,v)}\Big[\frac{s}{2}+r+1+\frac{k^2d}{2}+\mathsf{v}_2\Big(\frac{k}{v}\Big)\Big] \equiv 2Sy \bmod 4\,.$$

2. We want to apply 1., and to do so we must prove:

$$\textbf{A}.\quad 2 \,\Big|\, \frac{ku}{(k,v)} \quad \text{and} \quad 4 \,\Big|\, \frac{ksu}{(k,v)}\,; \qquad \textbf{B}.\quad S \equiv 0 \bmod 2\,.$$

Proof of **A.** If $2\nmid s$, then (a) implies

$$\mathsf{v}_2\Big(\frac{ku}{(k,v)}\Big) \ge \mathsf{v}_2(k)+\mathsf{v}_2(u)-\mathsf{v}_2(v)\ge 3\,, \quad \text{and thus} \quad 8\,\Big|\,\frac{ku}{(k,v)}\,\Big|\,\frac{ksu}{(k,v)}\,.$$

If $2\,|\,s$, then it suffices to prove the first assertion. If $2\,|\,u$, there is nothing to do. If $2\nmid u$, then (b) implies

$$\mathsf{v}_2\Big(\frac{ku}{(k,v)}\Big) \ge \mathsf{v}_2(k)+\mathsf{v}_2(u)-\mathsf{v}_2(v)\ge 1+\mathsf{v}_2(u)\ge 1\,, \quad \text{and thus} \quad 2\,\Big|\,\frac{ku}{(k,v)}\,.$$

Proof of **B.** We distinguish three cases.

CASE 1: $2\nmid s$. Then $\mathsf{v}_2(k)\ge \mathsf{v}_2(v)+3-\mathsf{v}_2(u)$ by (a), hence $8(k,v)\,|\,8v\,|\,ku$, and therefore

$$S=\frac{ksu}{4(k,v)}+\frac{ku}{2(k,v)}\Big[r+1+\frac{k^2d}{2}+\mathsf{v}_2(k)-\mathsf{v}_2(v)\Big]\equiv 0 \mod 2\,.$$

CASE 2: $2\,|\,s$ and $2\nmid u$. Then $\mathsf{v}_2(k)\ge 1+\mathsf{v}_2(v)$, hence $2(k,v)\,|\,2v\,|\,k$, $4\,|\,k^2d$, and

$$S\equiv\frac{ku}{2(k,v)}\Big[\frac{s}{2}+r+1+\mathsf{v}_2(k)-\mathsf{v}_2(v)\Big] \mod 2\,.$$

If $\mathsf{v}_2(k)\ge 2+\mathsf{v}_2(v)$, then $4(k,v)\,|\,4v\,|\,k$, and therefore $S\equiv 0 \mod 2$. Thus assume that $\mathsf{v}_2(k)=1+\mathsf{v}_2(v)$. Then (c), implies $4\,|\,2r+s$, hence

$$\frac{s}{2}+r+1+\mathsf{v}_2(k)-\mathsf{v}_2(v)\equiv\frac{2r+s}{2}+2\equiv 0 \mod 2\,,$$

and therefore again $S\equiv 0 \mod 2$.

CASE 3: $2\,|\,s$ and $2\,|\,u$. Clearly, $4\,|\,u$ implies $S\equiv 0 \mod 2$. Thus assume that $u\equiv 2 \mod 4$. Then $2\nmid v$, hence $2\nmid (k,v)$, and

$$S\equiv k\,\Big[\frac{s}{2}+r+1+\frac{k^2d}{2}+\mathsf{v}_2(k)\Big] \mod 2\,.$$

If $2\,|\,k$, then $S\equiv 0 \mod 2$. If $2\nmid k$, then $d+2r+s\equiv 2 \mod 4$ by (d), and thus again

$$S\equiv\frac{s+2r+2+d}{2}\equiv 0 \mod 2\,. \qquad\square$$

Theorem 7.6.2. *Let* $d,\,k,\,u,\,v\in\mathbb{Z}$ *be such that* $2\,|\,kd$, $dv(u^2-dv^2)\ne 0$, $(u,v)=1$, *and set* $u^2-dv^2=(-1)^r2^sW$, *where* $r\in\{0,1\}$, $s\in\mathbb{N}_0$, $W\in\mathbb{Z}$ *and* $W\equiv 1 \mod 4$. *Let* w *be the product of all primes dividing* W, *suppose that* $w\,|\,ku$, *and assume that the conditions* (a), (b), (c), (d) of Theorem 7.6.1.2 *are fulfilled.*

1. *There is a unique character* $\chi\colon\mathfrak{F}_{-4k^2d}\to\mathbb{C}^\times$ *such that*

$$\chi(F)=\Big(\frac{bv-ku\mathsf{i}}{a}\Big)_4\,,$$

whenever $F=[\![a,2b,c]\!]\in\mathfrak{F}_{-4k^2d}$, *where* $a\in\mathbb{N}$, $b,\,c\in\mathbb{Z}$, $b^2-ac=-k^2d$ *and* $(a,2b,c)=(a,2kd(u^2-dv^2))=1$ [*then* $(bv-ku\mathsf{i},a)=1$].

2. $\chi^4=\mathbf{1}$, *and if* u^2-dv^2 *and* $-d(u^2-dv^2)$ *are not squares, then* $\operatorname{ord}(\chi)=4$.

3. *Let p be a prime, $p \nmid 2kd(u^2-dv^2)$, $\varepsilon \in \{\pm 1\}$ such that $p \equiv \varepsilon \bmod 4$ and $t \in \mathbb{Z}$ such that $t^2 \equiv -d \bmod p$. Then*
$$\frac{u+vt\mathsf{i}}{-u+vt\mathsf{i}} \in D_{[p]}\,,$$
and p is represented by some class $F \in \mathfrak{F}_{-4k^2d}$ which satisfies
$$\chi(F) \equiv \Bigl(\frac{u+vt\mathsf{i}}{-u+vt\mathsf{i}}\Bigr)^{(p-\varepsilon)/4} \bmod p \quad \textit{or} \quad \overline{\chi}(F) \equiv \Bigl(\frac{u+vt\mathsf{i}}{-u+vt\mathsf{i}}\Bigr)^{(p-\varepsilon)/4} \bmod p\,.$$
In particular, p is represented by some class in $\mathrm{Ker}(\chi)$ if and only if
$$\Bigl(\frac{u+vt\mathsf{i}}{-u+vt\mathsf{i}}\Bigr)^{(p-\varepsilon)/4} \equiv 1 \bmod p\,.$$

PROOF. 1. If $F = [\![a,2b,c]\!] \in \mathfrak{F}_{-4k^2d}$, where $a \in \mathbb{N}$, $b,\,c \in \mathbb{Z}$, $b^2-ac=-k^2d$ and $(a,2b,c) = (a,2kd(u^2-dv^2)) = 1$, then
$$\mathcal{N}(bv-ku\mathsf{i}) = b^2v^2+k^2u^2 = (ac-k^2d)v^2+k^2u^2 \equiv k^2(u^2-dv^2) \bmod a\,,$$
and therefore $(a, bv-ku\mathsf{i}) = 1$. Since every class $F \in \mathfrak{F}_{-4k^2d}$ is of this form, the uniqueness of χ is obvious.

To prove existence, we show first that the definition suggested by the assertion of the theorem is independent from the chosen representatives. To be precise, we announce the following statement :

I. Assume that $a,\,b,\,c,\,a_1,\,b_1,\,c_1 \in \mathbb{Z}$ are such that $b^2-ac = b_1^2-a_1c_1 = -k^2d$, $(a,2b,c) = (a_1,2b_1,c_1) = 1$ and $(aa_1,\,2kd(u^2-dv^2)) = 1$. Then
$$[\![a,2b,c]\!] = [\![a_1,2b_1,c_1]\!] \quad \text{implies} \quad \Bigl(\frac{b_1v-ku\mathsf{i}}{a_1}\Bigr)_4 = \Bigl(\frac{bv-ku\mathsf{i}}{a}\Bigr)_4\,.$$

Proof of **I.** Suppose that $[a,2b,c] \sim [a_1,2b_1,c_1]$, say
$$[a_1,2b_1,c_1] = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} [a,2b,c]\,, \quad \text{where} \quad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathsf{SL}_2(\mathbb{Z})\,.$$
Then $a_1 = a\alpha^2+2b\alpha\beta+c\beta^2$, $b_1 = a\alpha\gamma+b(\alpha\delta+\beta\gamma)+c\beta\delta$ and $c_1 = a\gamma^2+2b\gamma\delta+c\delta^2$. It follows that $(a,\beta)\,|\,a_1$, and
$$\begin{aligned} b_1\beta &= a\alpha\beta\gamma+b\beta^2\gamma+b\alpha\beta\delta+\delta(a_1-a\alpha^2-2b\alpha\beta) \\ &\equiv a\alpha(\beta\gamma-\alpha\delta)+b\beta(\beta\gamma-\alpha\delta) \equiv -a\alpha-b\beta \bmod a_1\,. \end{aligned}$$
We define
$$x=\alpha\,, \quad y=\frac{\beta}{(a,\beta)}\,, \quad a^*=\frac{a}{(a,\beta)}\,, \quad a_1^*=\frac{a_1}{(a,\beta)} \quad \text{and} \quad c^*=(a,\beta)c\,.$$
Then $b^2-a^*c^* = b^2-ac = -k^2d$, $a^*x^2+2bxy+c^*y^2 = a_1^*$, $b_1y \equiv -a^*x-by \bmod a_1^*$, $(a^*,y) = (x,y) = 1$, and we assert that $(a_1^*,y) = 1$. Indeed,
$$(a_1^*,y) = \Bigl(\frac{a_1}{(a,\beta)},\frac{\beta}{(a,\beta)}\Bigr) = \frac{(a_1,\beta)}{(a,\beta)} \Bigm| \frac{a\alpha^2}{(a,\beta)} = a^*x^2\,,$$
hence $(a_1^*,y)\,|\,(a^*x^2,y) = (a^*,y) = 1$. It follows that $(a^*a_1^*,y) = 1$, and therefore
$$\bigl(a^*(a^*x^2+2bxy+c^*y^2),2ky(u^2-dv^2)\bigr) \bigm| \bigl(a^*a_1^*,2ky(u^2-dv^2)\bigr) \bigm| \bigl(aa_1,2kd(u^2-dv^2)\bigr)\,,$$

which implies

$$\big(a^*(a^*x^2+2bxy+c^*y^2),\,2ky(u^2-dv^2)\big)=1\,.$$

Also, $\mathcal{N}(bv-ku\mathsf{i})=b^2v^2+k^2u^2=(a^*c^*-k^2d)v^2+k^2u^2\equiv k^2(u^2-dv^2) \bmod a^*$, and therefore $(bv-ku\mathsf{i},a^*)=1$. By Theorem 7.6.1.2, it follows that

$$\Big(\frac{(a^*x+by)v+kuy\mathsf{i}}{a^*x^2+2bxy+c^*y^2}\Big)_4=\Big(\frac{bv-ku\mathsf{i}}{a^*}\Big)_4\,.$$

In the following calculations we use the congruences $-b_1y\equiv a^*x+by \bmod a'^*$ and $b_1\equiv b\alpha\delta\equiv b(1+\beta\gamma)\equiv b \bmod (a,\beta)$. So we obtain

$$\begin{aligned}\Big(\frac{b_1v-ku\mathsf{i}}{a'}\Big)_4&=\Big(\frac{b_1v-ku\mathsf{i}}{a'^*}\Big)_4\Big(\frac{b_1v-ku\mathsf{i}}{(a,\beta)}\Big)_4=\Big(\frac{b_1v-ku\mathsf{i}}{a'^*}\Big)_4\Big(\frac{-y}{a'^*}\Big)_4\Big(\frac{b_1v-ku\mathsf{i}}{(a,\beta)}\Big)_4\\&=\Big(\frac{-b_1vy+kuy\mathsf{i}}{a'^*}\Big)_4\Big(\frac{b_1v-ku\mathsf{i}}{(a,\beta)}\Big)_4=\Big(\frac{(a^*x+by)v+kuy\mathsf{i}}{a^*x^2+2bxy+c^*y^2}\Big)_4\Big(\frac{bv-ku\mathsf{i}}{(a,\beta)}\Big)_4\\&=\Big(\frac{bv-ku\mathsf{i}}{a^*}\Big)_4\Big(\frac{bv-ku\mathsf{i}}{(a,\beta)}\Big)_4=\Big(\frac{bv-ku\mathsf{i}}{a}\Big)_4,\end{aligned}$$

which completes the proof of **I.**

By **I.** there exists a map $\chi\colon\mathfrak{F}_{-4k^2d}\to\mathbb{C}^\times$ as asserted, and we must prove that χ is a homomorphism. Suppose that F_1, $F_2\in\mathfrak{F}_{-4k^2d}$. By Theorem 6.4.5 there exist a_1, $a_2\in\mathbb{N}$ and b, $c\in\mathbb{Z}$ such that $(a_1,a_2)=(a_1a_2,2kd(u^2-dv^2))=1$, $F_1=\llbracket a_1,2b,a_2c\rrbracket$, $F_2=\llbracket a_2,2b,a_1c\rrbracket$ and $F_1*F_2=(a_1a_2,2b,c)$. Hence we obtain

$$\chi(F_1*F_2)=\Big(\frac{bv-ku\mathsf{i}}{a_1a_2}\Big)_4=\Big(\frac{bv-ku\mathsf{i}}{a_1}\Big)_4\Big(\frac{bv-ku\mathsf{i}}{a_2}\Big)_4=\chi(F_1)\chi(F_2)\,.$$

2. By definition, $\chi^4=\mathbf{1}$. Hence suppose that u^2-dv^2 and $-d(u^2-dv^2)$ are not squares. We must prove that $\chi(F)^2=-1$ for some class $F=\llbracket p,2kx,k^2y\rrbracket\in\mathfrak{F}_{-4k^2d}$. By the subsequent Lemma 7.6.3 there exists a prime p such that $p\nmid 2kd(u^2-dv^2)$ and

$$\Big(\frac{u^2-dv^2}{p}\Big)=\Big(\frac{-d(u^2-dv^2)}{p}\Big)=-1\,,\quad\text{ and therefore }\quad\Big(\frac{-d}{p}\Big)=1\,.$$

Let x, $y\in\mathbb{Z}$ be such that $x^2=-d+py$. Then $p\nmid x$, hence $(p,2kx,k^2y)=1$, $(2px)^2-4pk^2y^2=-4k^2d$, and $F=\llbracket p,2kx,k^2y\rrbracket\in\mathfrak{F}_{-4k^2d}$. By Theorem 7.3.9.1, we obtain

$$\chi^2(F)=\Big(\frac{kxv-ku\mathsf{i}}{p}\Big)_2=\Big(\frac{k^2x^2v^2+k^2u^2}{p}\Big)=\Big(\frac{u^2-dv^2}{p}\Big)=-1\,.$$

3. Since $u^2+v^2t^2\equiv u^2-v^2d\not\equiv 0 \bmod p$, it follows (observing Theorem and Definition A.8.5) that

$$\frac{u+vt\mathsf{i}}{-u+vt\mathsf{i}}=\frac{-(u+vt\mathsf{i})^2}{u^2+v^2t^2}\in D_{[p]}\,.$$

By definition, we have

$$\mathsf{Q}_{-4k^2d}(p)=\Big(\frac{-4k^2d}{p}\Big)=\Big(\frac{-d}{p}\Big)=1\,,$$

and, by Theorem 6.4.13.2, p is represented by some class $F = \llbracket p, 2b, c \rrbracket \in \mathfrak{F}_{-4k^2d}$, where $b,\ c \in \mathbb{Z}$, $(p, 2b, c) = 1$, $b^2 - pc = -k^2d$, and

$$\chi(F) = \Big(\frac{bv - ku\mathsf{i}}{p}\Big)_4 .$$

CASE 1: $p \,|\, u$. In this case, the assertion follows since

$$\chi(F) = \Big(\frac{bv}{p}\Big)_4 = 1 \quad \text{and} \quad \frac{u + vt\mathsf{i}}{-u + vt\mathsf{i}} \equiv 1 \mod p .$$

CASE 2: $p \nmid u$. Since $b^2 \equiv -k^2d \equiv k^2t^2 \mod p$, there exists some $\delta \in \{\pm 1\}$ such that $b \equiv \delta kt \mod p$. Let $w \in \mathbb{Z}$ be such that $uw \equiv v \mod p$. Then we obtain

$$bv - ku\mathsf{i} \equiv \delta ktuw - ku\mathsf{i} \equiv -ku(-\delta kw + \mathsf{i}) \mod p ,$$

$$u(-\delta tw \pm \varepsilon\mathsf{i}) \equiv -\delta vt \pm u\varepsilon\mathsf{i} \equiv \varepsilon\mathsf{i}(\pm u + \varepsilon\delta vt\mathsf{i}) \mod p ,$$

and by Theorem 7.3.9.2 we get

$$\begin{aligned}\chi(F) = \Big(\frac{bv - ku\mathsf{i}}{p}\Big)_4 = \Big(\frac{-ku}{p}\Big)_4 \Big(\frac{-\delta tw + \mathsf{i}}{p}\Big)_4 &\equiv \Big(\frac{-\delta tw + \varepsilon\mathsf{i}}{-\delta tw - \varepsilon\mathsf{i}}\Big)^{(p-\varepsilon)/4} \\ &\equiv \Big(\frac{u + \varepsilon\delta vt\mathsf{i}}{-u + \varepsilon\delta vt\mathsf{i}}\Big)^{(p-\varepsilon)/4} \mod p .\end{aligned}$$

Now the assertion follows immediately if $\varepsilon\delta = 1$, and if $\varepsilon\delta = -1$, it follows since

$$\frac{u - vt\mathsf{i}}{-u - vt\mathsf{i}} = \overline{\frac{u + vt\mathsf{i}}{-u + vt\mathsf{i}}} . \qquad \square$$

Lemma 7.6.3. *Let $u,\ v \in \mathbb{Z}$ be not squares. Then there exist infinitely many primes p such that*

$$p \nmid 2uv \quad \textit{and} \quad \Big(\frac{u}{p}\Big) = \Big(\frac{v}{p}\Big) = -1 .$$

PROOF. It suffices to prove that there exists some $x \in \mathbb{Z}$ such that

$$(x, 2uv) = 1 \quad \text{and} \quad \Big(\frac{u}{x}\Big) = \Big(\frac{v}{x}\Big) = -1 .$$

Indeed, once this is done, then (by Dirichlet's prime number theorem) there exist infinitely many primes $p \equiv x \mod 4uv$, and these have the desired properties. We prove first:

A. If $d \in \mathbb{Z}$ is not a square and $k \in \mathbb{N}$, then there exists some $x \in \mathbb{N}$ such that

$$(x, 2dk) = 1 \quad \text{and} \quad \Big(\frac{d}{x}\Big) = -1 .$$

Proof of **A.** By Theorem 3.5.5.1, Q_{4d} is a quadratic character, and thus there exists some $y \in \mathbb{Z}$ such that $(y, 2d) = 1$ and $\mathsf{Q}_{4d}(y) = -1$. If $x \in \mathbb{N}$, $x \equiv y \mod 4d$ and $(x, k) = 1$, then $(x, 2kd) = 1$ and

$$\Big(\frac{d}{x}\Big) = \Big(\frac{4d}{x}\Big) = \Big(\frac{4d}{y}\Big) = \mathsf{Q}_{4d}(y) = -1 . \qquad \square[\mathbf{A}.]$$

By **A**, we may assume that u and v are distinct and squarefree, say

$$u = (-1)^\alpha 2^\beta dp_1 \cdot \ldots \cdot p_r \quad \text{and} \quad v = (-1)^\gamma 2^\delta dq_1 \cdot \ldots q_s ,$$

where $\alpha,\ \beta,\ \gamma,\ \delta \in \{0,1\}$, $r,\ s \in \mathbb{N}_0$, $r \ge s$, $d \in \mathbb{N}$ is odd and squarefree, and $p_1,\ldots,p_r,\ q_1,\ldots,q_s$ are distinct odd primes not dividing d.

CASE 1: $d>1$. If $x \in \mathbb{N}$ is such that

$$x \equiv 1 \mod 8p_1\cdot\ldots\cdot p_rq_1\cdot\ldots\cdot q_s \quad\text{and}\quad \Big(\frac{x}{d}\Big) = -1\,,$$

then

$$\Big(\frac{u}{x}\Big) = \Big(\frac{(-1)^\alpha 2^\beta}{x}\Big)\Big(\frac{d}{x}\Big)\Big(\frac{p_1\cdot\ldots\cdot p_r}{x}\Big) = \Big(\frac{d}{x}\Big) = \Big(\frac{x}{d}\Big) = -1\,,\quad\text{and alike}\quad \Big(\frac{v}{x}\Big) = -1\,.$$

CASE 2: $d=1$ and $r>0$. By **A**, there exists some $y \in \mathbb{N}$ such that

$$(y,2uv)=1 \quad\text{and}\quad \Big(\frac{v}{y}\Big) = -1\,.$$

If $x \in \mathbb{N}$ is such that

$$x \equiv y \mod 8vp_1\cdot\ldots\cdot p_{r-1}\,,\quad p_r \nmid x \quad\text{and}\quad \Big(\frac{x}{p_r}\Big) = -\Big(\frac{p_r^{-1}u}{y}\Big)(-1)^{\frac{p_r-1}{2}\frac{y-1}{2}}\,,$$

then $(x,2uv)=1$, $x \equiv y \mod 4p_r^{-1}uv$,

$$\begin{aligned}\Big(\frac{u}{x}\Big) &= \Big(\frac{p_r^{-1}u}{x}\Big)\Big(\frac{p_r}{x}\Big) = \Big(\frac{p_r^{-1}u}{y}\Big)(-1)^{\frac{p_r-1}{2}\frac{x-1}{2}}\Big(\frac{x}{p_r}\Big)\\ &= \Big(\frac{p_r^{-1}u}{y}\Big)(-1)^{\frac{p_r-1}{2}\frac{y-1}{2}}\Big(\frac{x}{p_r}\Big) = -(-1)^{\frac{p_r-1}{2}\left(\frac{x-1}{2}+\frac{y-1}{2}\right)} = -1\end{aligned}$$

and

$$\Big(\frac{v}{x}\Big) = \Big(\frac{v}{y}\Big) = -1\,.$$

CASE 3: $d=1$ and $r=0$. If

$$x = \begin{cases} 3 & \text{if}\ \ \{u,v\}=\{-1,2\}\,,\\ 7 & \text{if}\ \ \{u,v\}=\{-1,-2\}\,,\\ 5 & \text{if}\ \ \{u,v\}=\{2,-2\}\,,\end{cases}\quad\text{then}\quad \Big(\frac{u}{x}\Big) = \Big(\frac{v}{x}\Big) = -1\,. \qquad \square$$

Theorem 7.6.4. *Suppose that* $m=2^\alpha m_0$, *where* $\alpha \in \mathbb{N}_0$ *and* $m_0 \in \mathbb{Z}\setminus 2\mathbb{Z}$. *Let* m_1 *be the product of all primes dividing* m_0 *and*

$$k = \begin{cases} 8m_1 & \textit{if}\ \ 2\nmid\alpha\,,\\ 4m_1 & \textit{if}\ \ m_0-\alpha \equiv 3 \mod 4\,,\\ 2m_1 & \textit{if}\ \ m_0-\alpha\equiv 1 \mod 4\,.\end{cases}$$

Then there is a unique character $\varphi\colon \mathfrak{F}_{-4k^2} \to \mathbb{C}^\times$ *such that*

$$\varphi(F) = \Big(\frac{(m+1)b-(m-1)k\mathsf{i}}{a}\Big)_4\,,$$

whenever $F = [\![a,2b,c]\!] \in \mathfrak{F}_{-4k^2}$, *where* $a \in \mathbb{N}$, $b,\ c \in \mathbb{Z}$, $(a,2b,c)=(a,m)=1$ *and* $b^2-ac=-k^2$ [*then* $((m+1)b-(m-1)k\mathsf{i},a)=1$]. *It satisfies* $\varphi^4 = \mathbf{1}$, *and* $\operatorname{ord}(\varphi)=4$ *if* $|m|$ *is not a square.*

If $p \equiv 1 \bmod 4$ *is a prime such that* $p\nmid m$, *then* m *is a biquadratic residue modulo* p *if and only if* m *is represented by some class* $F \in \operatorname{Ker}(\varphi)$.

PROOF. Let $p \equiv 1 \bmod 4$ be a prime such that $p \nmid m$. Then $p \nmid k$, by Theorem 6.4.13.2 p is represented by some class $F \in \mathfrak{F}_{-4k^2}$, and then F and F^{-1} are the only classes which represent p. Since every class $F \in \mathfrak{F}_{-4k^2}$ is of the form $F = [\![a, 2b, c]\!]$, where $a \in \mathbb{N}$, $b, c \in \mathbb{Z}$, $(a, 2b, c) = 1$ and $b^2 - ac = -k^2$, the uniqueness of φ follows.

We apply Theorem 7.6.2 with $d = 1$, $t = -\mathsf{i}$ and k as defined above.

CASE 1: $m \equiv 0 \bmod 2$. We set $u = m - 1$ and $v = m + 1$. Then $(u, v) = 1$, and $u^2 - v^2 = -4m = (-1)^r 2^s W$, where $s = 2 + \alpha$, $r = 0$ if $m \equiv 3 \bmod 4$, $r = 1$ if $m \equiv 1 \bmod 4$, $W = (-1)^{r+1} m_0 \equiv 1 \bmod 4$ and $w = m_1$.

We check the conditions (a), (b), (c), (d) of Theorem 7.6.1.2. Since $2 \nmid uv$ and $2 \,|\, k$, (b) and (d) hold. If $2 \nmid s$, then $2 \nmid \alpha$ and $8 \,|\, k$, hence (a) holds since $\mathsf{v}_2(k) \geq 3 = \mathsf{v}_2(v) + \max\{3 - \mathsf{v}_2(u), 0\}$. It remains to consider the case where $2 \,|\, s$ and $4 \nmid 2r + s$. In this case, $2r + s = 2r + \alpha + 2$, and therefore $2r + \alpha \equiv 0 \bmod 4$. If $m_0 \equiv 1 \bmod 4$, then $r = 1$, $4 \nmid \alpha$, and consequently $m_0 - \alpha \equiv 3 \bmod 4$ and $4 \,|\, k$. If $m_0 \equiv 3 \bmod 4$, then $r = 0$, $4 \,|\, \alpha$, and thus again $m_0 - \alpha \equiv 3 \bmod 4$ and $4 \,|\, k$.

By Theorem 7.6.2 there exists a unique character $\chi \colon \mathfrak{F}_{-4k^2} \to \mathbb{C}^\times$ such that

$$\chi(F) = \Big(\frac{bv - ku\mathsf{i}}{a}\Big)_4 = \Big(\frac{(m+1)b - (m-1)k\mathsf{i}}{a}\Big)_4$$

for every class $F = [\![a, 2b, c]\!] \in \mathfrak{F}_{-4k^2}$ as above, and we set $\varphi = \chi$. Then $\varphi^4 = \mathbf{1}$, and if $|m|$ is not a square, then $\mathrm{ord}(\varphi) = 4$. If F represents p, then $\varphi(F) = 1$ if and only if

$$\Big(\frac{u + v}{-u + v}\Big)^{(p-1)/4} = \Big(\frac{m - 1 + (m+1)}{-(m-1) + (m+1)}\Big)^{(p-1)/4} = m^{(p-1)/4} \equiv 1 \bmod p\,.$$

Hence m is a biquadratic residue modulo p if and only if p is represented by some class $F \in \mathrm{Ker}(\varphi)$ (indeed, if some class $F \in \mathfrak{F}_{-4k^2}$ represents p, then F and F^{-1} are the only classes in $\mathfrak{F}_{-4k^2}$ which represent p).

CASE 2: $\varepsilon \in \{\pm 1\}$ and $m \equiv \varepsilon \bmod 4$. Suppose that $m - \varepsilon = 2u$ and $m + \varepsilon = 2v$, where $u, v \in \mathbb{Z}$, $4 \,|\, u$, $2 \nmid v$ and $(u, v) = 1$. We set $u^2 - v^2 = -\varepsilon m = (-1)^r 2^s W$, where $s = 0$, $r = 1$, $W = \varepsilon m \equiv 1 \bmod 4$ and $w = m_1$. Since $2 \,|\, k$, the conditions (a), (b), (c), (d) of Theorem 7.6.1 are obviously satisfied.

By Theorem 7.6.2 there exists a unique character $\chi \colon \mathfrak{F}_{-4k^2} \to \mathbb{C}^\times$ such that

$$\chi(F) = \Big(\frac{bv - ku\mathsf{i}}{a}\Big)_4 = \Big(\frac{bv - ku\mathsf{i}}{a}\Big)_4 \Big(\frac{2}{a}\Big)_4 = \Big(\frac{(m+\varepsilon)b - (m-\varepsilon)k\mathsf{i}}{a}\Big)_4$$

for every class $F = [\![a, 2b, c]\!] \in \mathfrak{F}_{-4k^2}$ as above. Since

$$\frac{u + vt\mathsf{i}}{-u + vt\mathsf{i}} = \frac{u + v}{-u + v} = \varepsilon m \quad \text{and} \quad \overline{\varepsilon m} = \varepsilon m\,,$$

it follows that F represents p if and only if $\chi(F) \equiv (\varepsilon m)^{(p-1)/4} \bmod p$.

If $\varepsilon = 1$ and $m \equiv 1 \bmod 4$, then we set $\varphi = \chi$ and proceed as in CASE 1. Thus suppose that $\varepsilon = -1$, $m \equiv 3 \bmod 4$, and consequently $-4k^2 \equiv 0 \bmod 32$. Let $\delta \colon \mathfrak{F}_{-4k^2} \to \{\pm 1\}$ be the basic genus character defined by

$$\delta(F) = \Big(\frac{2}{a}\Big) \quad \text{if } F = [\![a, 2b, c]\!] \in \mathfrak{F}_{-4k^2} \text{ is as above, and set } \varphi = \delta\chi.$$

Since $\delta^2 = \mathbf{1}$, it follows that $\varphi^4 = \mathbf{1}$, and $\operatorname{ord}(\varphi) = 4$ if $|m|$ is not a square. If $F \in \mathfrak{F}_{-4k^2}$ as above represents p, then $p \equiv 1 \bmod 4$, hence $\delta(F) = (-1)^{(p-1)/4}$, and

$$\varphi(F) = \delta(F)\chi(F) \equiv (-1)^{(p-1)/4}(-m)^{(p-1)/4} \equiv m^{(p-1)/4} \mod p\,.$$

Therefore m is a biquadratic residue modulo p if and only if p is represented by some class $F \in \operatorname{Ker}(\varphi)$. □

Example 7.6.5. For $m \in \mathbb{Z}$ with $1 < |m| \le 10$ we present a list of quadratic forms $[a, b, c]$ with the following property:

m is a biquadratic residue modulo a prime $p \equiv 1 \bmod 4$ with $p \nmid m$ if and only if p is represented by some form in the list.

$m = \pm 2$: $[1,0,64]$;

$m = 3$: $[1,0,144]$, $[13,10,13]$;

$m = -3$: $[1,0,36]$;

$m = 5$: $[1,0,100]$;

$m = -5$: $[1,0,400]$, $[16,16,29]$;

$m = 6$: $[1,0,576]$, $[25,14,25]$, $[5,\pm4,116]$;

$m = -6$: $[1,0,576]$, $[25,14,25]$, $[20,\pm4,29]$;

$m = 7$: $[1,0,784]$, $[16,0,49]$, $[29,\pm24,32]$;

$m = -7$: $[1,0,196]$, $[4,0,49]$;

$m = 10$: $[1,0,1600]$, $[41,18,41]$, $[37,\pm36,52]$;

$m = -10$: $[1,0,1600]$, $[41,18,41]$, $[13,\pm10,125]$.

We give the details for $m = 6$. In this case, $\alpha = 1$, $m_0 = m_1 = 3$, $k = 24$ and $-4k^2 = -2304$. There exist 16 reduced forms of discriminant -2304:

$[1,0,576]$, $[9,0,64]$, $[4,4,145]$, $[5,\pm4,116]$, $[20,\pm4,29]$, $[9,\pm6,65]$, $[13,\pm6,45]$, $[16,\pm8,37]$, $[17,\pm12,36]$, $[25,14,25]$

(see http://www.numbertheory.org/php/classnoneg.php).

The class group is given by $\mathfrak{F}_{-2304} = \langle A, C\rangle$, where $A = [\![5,4,116]\!]$, $C = [\![9,6,65]\!]$ and $\operatorname{ord}(A) = \operatorname{ord}(C) = 4$. Since

$$\varphi(A) = \Big(\frac{7\cdot 2 - 5\cdot 24\mathrm{i}}{5}\Big)_4 = \Big(\frac{14}{5}\Big)_4 = 1\,,$$

it follows that $A \in \operatorname{Ker}(\varphi)$, and since $(\mathfrak{F}_{-2304} : \operatorname{Ker}(\varphi)) = 4$, we obtain

$$\operatorname{Ker}(\varphi) = \langle A\rangle = \{A,\, A^2,\, A^3,\, A^4 = I\} = \{\, [\![5,\pm4,116]\!],\ [\![25,14,25]\!],\ [\![1,0,576]\!]\,\}\,.$$

Theorem 7.6.6. *Let Δ be a quadratic discriminant, let $m,\,n,\,q \in \mathbb{Z}$ be non-zero integers such that $(m,n)\,|\,2$, $q \equiv 1 \bmod 4$ and $m^2 - \Delta n^2 = -4q$. Let q_1 be the product of all primes dividing q,*

$$\alpha = \frac{m + n\sqrt{\Delta}}{2} \quad \text{and} \quad k = \begin{cases} q_1 & \text{if } \ \Delta \equiv 4 \bmod 8\,, \\ 2q_1 & \text{otherwise}\,. \end{cases}$$

Then there is a unique character $\chi\colon \mathfrak{F}_{-4k^2\Delta} \to \mathbb{C}^\times$ *such that*

$$\chi(F) = \Bigl(\frac{bn - km\mathrm{i}}{a}\Bigr)_4,$$

whenever $F = [\![a, 2b, c]\!] \in \mathfrak{F}_{-k^2\Delta}$, *where* $a \in \mathbb{N}$, $b, c \in \mathbb{Z}$, $(a, 2b, c) = (a, 2\Delta q) = 1$ *and* $b^2 - ac = -\Delta k^2$ [*then* $(bv - km\mathrm{i}, a) = 1$]. *It satisfies* $\chi^4 = \mathbf{1}$, $\mathrm{ord}(\chi) = 4$ *if* $-q$ *and* Δq *are not squares, and it has the following properties*:

1. *If* $F = [\![a, 2b, c]\!] \in \mathfrak{F}_{-4k^2\Delta}$ *is as above and* $F \in \mathrm{Ker}(\chi)$, *then*
$$\Bigl(\frac{-q}{a}\Bigr) = 1\,.$$
2. *Let* $p \equiv 1 \bmod 4$ *be a prime such that* $p \nmid \Delta q$, *and* $-q$ *and* Δ *are both quadratic residues modulo* p. *Then*
$$\Bigl(\frac{\alpha}{p}\Bigr) = \Bigl[\frac{q}{p}\Bigr]_4 \quad \textit{if and only if } p \textit{ is represented by some class } F \in \mathrm{Ker}(\varphi).$$

PROOF. We apply Theorem 7.6.2 with k as above,

$$d = \Delta, \quad u = \frac{m}{(m,n)} \quad \text{and} \quad v = \frac{n}{(m,n)}\,.$$

Then $2 \,|\, k\Delta$, $(u, v) = 1$, and $\Delta v(u^2 - \Delta v^2) \ne 0$. We set $W = q$, $w = q_1$, $r = 1$, $s = 2$ if $(m, n) = 1$, and $s = 0$ if $(m, n) = 2$. Then

$$u^2 - dv^2 = \frac{-4q}{(m,n)^2} = (-1)^r 2^s W\,,$$

and we check the conditions (a), (b), (c), (d) of Theorem 7.6.1.

CASE 1: $\Delta \equiv 0 \bmod 8$. Then $m = 2m_0$ and $\Delta = 8D$, where $m_0, D \in \mathbb{Z}$ and $2 \nmid m_0$. It follows that $m_0^2 - 2Dn^2 = -q \equiv 3 \bmod 4$, hence $2 \nmid n$, $(m, n) = 1$, $2 \,|\, u$, and (d) holds since $2 \,|\, k$.

CASE 2: $\Delta \equiv 4 \bmod 8$. Then $m = 2m_0$ and $\Delta = 8D + 4$, where $m_0, D \in \mathbb{Z}$. It follows that $m_0^2 - (2d_0 + 1)n^2 = -q \equiv 3 \bmod 4$, hence $2 \,|\, m_0$, $4 \,|\, m$, $2 \nmid n$, $(m, n) = 1$ and $4 \,|\, u$. In this case there is no further condition to be checked.

CASE 3: $\Delta \equiv 1 \bmod 4$. Then $m^2 - n^2 \equiv 0 \bmod 4$, and thus $m \equiv n \bmod 2$. If $m \equiv n \equiv 1 \bmod 2$, then $u = m$, $v = n$, $2 \,|\, k$ and $2r + s = 4$. Hence the conditions (c) and (d) hold. If $m \equiv n \equiv 0 \bmod 2$, then $m = 2u$, $n = 2v$, $u^2 - v^2 \equiv -q \equiv 3 \bmod 4$, and therefore $2 \,|\, u$. Hence condition (d) holds since $2 \,|\, k$.

By Theorem 7.6.2, there exists a unique character $\chi\colon \mathfrak{F}_{-4k^2\Delta} \to \mathbb{C}^\times$ such that

$$\chi([\![a, 2b, c]\!]) = \Bigl(\frac{bv - ku\mathrm{i}}{a}\Bigr)_4,$$

whenever $a \in \mathbb{N}$, $b, c \in \mathbb{Z}$, $(a, 2b, c) = (a, 2k\Delta(u^2 - \Delta v^2)) = 1$ and $b^2 - ac = -k^2\Delta$ [then $(bv - ku\mathrm{i}, a) = 1$]. It satisfies $\chi^4 = \mathbf{1}$ and $\mathrm{ord}(\chi) = 4$ if $u^2 - \Delta v^2$ and $-\Delta(u^2 - \Delta v^2)$ are not squares. Now the existence and uniqueness of χ as asserted follows, since $(a, 2kq(u^2 - \Delta v^2)) = 1$ holds if and only if $(a, 2\Delta q) = 1$, $(bv - ku\mathrm{i}, a) = 1$ implies $(bn - km\mathrm{i}, a) = 1$ (as $2 \nmid a$), and

$$\Bigl(\frac{bv - ku\mathrm{i}}{a}\Bigr)_4 = \Bigl(\frac{bv - ku\mathrm{i}}{a}\Bigr)_4 \Bigl(\frac{(m,n)}{a}\Bigr)_4 = \Bigl(\frac{bn - kmu\mathrm{i}}{a}\Bigr)_4.$$

1. If $F=[\![a,2b,c]\!]\in\operatorname{Ker}(\chi)$, then Theorem 7.3.9.1 implies

$$1=\Bigl(\frac{bn-km\mathsf{i}}{a}\Bigr)_4^2=\Bigl(\frac{bn-km\mathsf{i}}{a}\Bigr)_2=\Bigl(\frac{b^2n^2+k^2m^2}{a}\Bigr)$$
$$=\Bigl(\frac{(ac-k^2d)n^2+k^2m^2}{a}\Bigr)=\Bigl(\frac{k^2(m^2-dn^2)}{a}\Bigr)=\Bigl(\frac{-q}{a}\Bigr).$$

2. Since both Δ and $\mathcal{N}(\alpha)=-q$ are quadratic residues modulo p, the generalized quadratic symbol is defined, and since $p\equiv 1\mod 4$, it follows that q is a quadratic residue modulo p, too. Let $\sigma,\ \vartheta\in\mathbb{Z}$ be such that $\sigma^2\equiv q\mod p$ and $\vartheta^2\equiv d\mod p$. By Theorem 6.4.13.2, p is represented by some class $F=[\![a,2b,c]\!]\in\mathfrak{F}_{-4k^2\Delta}$, where $a\in\mathbb{N}$, $b,\ c\in\mathbb{Z}$, $(a,2b,c)=1$, $b^2-ac=-k^2\Delta$ and $(a,2\Delta k)=1$. We apply Theorem 7.6.2 with $t=-\mathsf{i}\vartheta$ and obtain

$$\chi(F)=1\quad\text{if and only if}\quad Y=\Bigl(\frac{u+v\vartheta}{-u+v\vartheta}\Bigr)^{(p-1)/4}\equiv 1\mod p\,.$$

Since F and F^{-1} are the only classes in $\mathfrak{F}_{-4k^2\Delta}$ which represent p, it follows that p is represented by some class $F\in\operatorname{Ker}(\chi)$ if and only if $Y\equiv 1\bmod p$. Now we calculate

$$Y=\Bigl(\frac{u+v\vartheta}{-u+v\vartheta}\Bigr)^{(p-1)/4}=\Bigl(\frac{m+n\vartheta}{-m+n\vartheta}\Bigr)^{(p-1)/4}\equiv\Bigl(\frac{(m+n\vartheta)^2}{4q}\Bigr)^{(p-1)/4}$$
$$=\Bigl(\frac{m+n\vartheta}{2}\Bigr)^{(p-1)/2}q^{-(p-1)/4}\equiv\Bigl(\frac{\alpha}{p}\Bigr)\Bigl[\frac{q}{p}\Bigr]_4\mod p\,,$$

and we obtain

$$Y\equiv 1\mod p\quad\text{if and only if}\quad\Bigl(\frac{\alpha}{p}\Bigr)=\Bigl[\frac{q}{p}\Bigr]_4\,.\qquad\square$$

Corollary 7.6.7. *Let Δ be a quadratic discriminant and $m,\ n\in\mathbb{Z}$ such that $m^2-dn^2=-4$,*

$$\varepsilon=\frac{m+n\sqrt{\Delta}}{2}\,,\quad\textit{and}\quad k=\begin{cases}1 & \textit{if}\quad\Delta\equiv 4\mod 8\,,\\ 2 & \textit{otherwise}\,.\end{cases}$$

Then there is a unique character $\chi\colon\mathfrak{F}_{-4k^2\Delta}\to\mathbb{C}^\times$ such that

$$\chi(F)=\Bigl(\frac{bn-km\mathsf{i}}{a}\Bigr)_4\,,$$

whenever $F=[\![a,2b,c]\!]$, where $a\in\mathbb{N}$, $b,\ c\in\mathbb{Z}$, $(a,2b,c)=(a,2\Delta)=1$ and $b^2-ac=-k^2$. It satisfies $\operatorname{ord}(\varphi)=4$, and if some class $[\![a,2b,c]\!]$ as above lies in $\operatorname{Ker}(\chi)$, then $a\equiv 1\mod 4$.

If $p\equiv 1\mod 4$ is a prime such that $\mathsf{Q}_\Delta(p)=1$, then

$$\Bigl(\frac{\varepsilon}{p}\Bigr)=1\quad\textit{if and only if } p \textit{ is represented by some class } F\in\operatorname{Ker}(\varphi).$$

Proof. By Theorem 7.6.6, applied with $q=1$. $\square$

Example 7.6.8. For some fundamental discriminants $\Delta \in \mathbb{N}$ with $\mathcal{N}(\varepsilon_\Delta) = -1$ we present a list of quadratic forms f such that ε_Δ is a quadratic residue modulo a prime $p \equiv 1 \bmod 4$ with $\mathsf{Q}_\Delta(p) = 1$ if and only if p is represented by some form in the list.

$$\begin{aligned}
\Delta = 5\,,\ \varepsilon_5 = \frac{1+\sqrt{5}}{2}\ &: \quad [1,0,20]\,;\\
\Delta = 8\,,\ \varepsilon_8 = 1+\sqrt{2}\ &: \quad [1,0,32]\,;\\
\Delta = 13\,,\ \varepsilon_{13} = \frac{3+\sqrt{13}}{2}\ &: \quad [1,0,52]\,;\\
\Delta = 17\,,\ \varepsilon_{17} = 4+\sqrt{17}\ &: \quad [1,0,68]\,,\ [4,0,17];\\
\Delta = 29\,,\ \varepsilon_{29} = \frac{5+\sqrt{29}}{2}\ &: \quad [1,0,116]\,,\ [5,\pm 4,24]\,;\\
\Delta = 37\,,\ \varepsilon_{37} = 6+\sqrt{37}\ &: \quad [1,0,148]\,;\\
\Delta = 40\,,\ \varepsilon_{40} = 3+\sqrt{10}\ &: \quad [1,0,160]\,,\ [13,6,13]\,.
\end{aligned}$$

We give the details for $\Delta = 17$. Here $-4k^2\Delta = -272$, $m = 8$ and $n = 2$. There exist eight reduced forms of discriminant -272:

$[1,0,68]\,,\ [4,0,17]\,,\ [3,\pm 2,23]\,,\ [8,\pm 4,9]\,,\ [7,\pm 6,11]$

(see http://www.numbertheory.org/php/classnoneg.php).

The class group is given by $\mathfrak{F}_{-272} = \langle A, B\rangle$, where $A = [\![3,2,23]\!]$, $B = [\![4,0,17]\!]$, $\mathrm{ord}(A) = 4$ and $\mathrm{ord}(B) = 2$. Since $B = [\![17,0,4]\!]$, we obtain

$$\varphi(B) = \Big(\frac{-16\mathsf{i}}{17}\Big)_4 = \Big(\frac{\mathsf{i}}{17}\Big)_4 = 1\,,$$

hence $B \in \mathrm{Ker}(\varphi)$, and since $(\mathfrak{F}_{-272}\!:\!\mathrm{Ker}(\varphi)) = 4$, we obtain

$$\mathrm{Ker}(\varphi) = \langle B\rangle = \{B,\ B^2 = I\} = \{\,[\![4,0,17]\!],\ [\![1,0,68]\!]\,\}\,.$$

Remarks 7.6.9 (For readers who are familiar with class field theory)**.**

1. If $m \in \mathbb{Z}$, then Theorem 7.6.4 gives an explicit formula for the defining character of the cyclic field extension $\mathbb{Q}(\mathsf{i}, \sqrt[4]{m})/\mathbb{Q}(\mathsf{i})$.
2. If $\Delta \in \mathbb{N}$ is a fundamental discriminant such that $\mathcal{N}(\varepsilon_\Delta) = -1$, then Corollary 7.6.7 gives an explicit formula for the defining character of the cyclic field extension $\mathbb{Q}(\sqrt{\varepsilon}\,, \mathsf{i})/\mathbb{Q}(\sqrt{-\Delta}\,)$.

This page intentionally left blank

CHAPTER 8

Class groups

Let Δ be a quadratic discriminant. In Chapter 1 we introduced the class number h_Δ and the narrow class number h_Δ^+ in terms of equivalent quadratic irrationals, and in Chapter 5 we interpreted these numbers as ideal class numbers of quadratic orders, namely

$$h_\Delta = |\mathcal{C}_\Delta| \quad \text{and} \quad h_\Delta^+ = |\mathcal{C}_\Delta^+|\,.$$

There we proved:

- If $\Delta < 0$, then $\mathcal{C}_\Delta = \mathcal{C}_\Delta^+$.
- If $\Delta > 0$, then there is a natural epimorphism $\mathcal{C}_\Delta^+ \to \mathcal{C}_\Delta$, and

$$h_\Delta^+ = \frac{2h_\Delta}{(\mathcal{O}_\Delta^\times : \mathcal{O}_\Delta^{\times +})} = \begin{cases} h_\Delta & \text{if} \quad \mathcal{N}(\varepsilon_\Delta) = -1\,, \\ 2h_\Delta & \text{if} \quad \mathcal{N}(\varepsilon_\Delta) = 1\,, \end{cases}$$

  where $\mathcal{O}_\Delta^{\times +} = \{\varepsilon \in \mathcal{O}_\Delta^\times \mid \mathcal{N}(\varepsilon) = 1\}$ is the group of norm-positive units.

In Chapter 6, we established an isomorphism

$$\mathfrak{F}_\Delta \overset{\sim}{\to} \mathcal{C}_\Delta^+$$

between the narrow ideal class group $\mathcal{C}_\Delta^+$ and Gauss' composition class group $\mathfrak{F}_\Delta$ of binary quadratic forms.

Consequently, equivalence classes of quadratic irrationals, ideal class groups of quadratic orders and composition class groups of binary forms constitute equivalent theories, and it is a matter of taste and convenience to describe the theory in terms of quadratic irrationals, ideals or forms.

In this final chapter, we first deal with the analytic theory of quadratic orders. In Section 8.1, we prove Dirichlet's analytic class number formula and draw some of its consequences. In Section 8.2 we introduce L-functions of quadratic orders, reconsider the analytic class number formula and prove the quadratic analog of Dirichlet's prime number theorem. In these two sections we tacitly use the results of Chapter 4.

The remaining two sections are devoted to the 2-component of the class group of a quadratic order, called its 2-*class group*. We translate the theory of ambiguous ideals into the language of forms, and then we concentrate on cyclic 2-class groups. We provide criteria for a cyclic 2-class group to be of an order divisible by 4, 8 or 16.

8.1. The analytic class number formula

The main idea for the proof of Dirichlet's class number formula is an asymptotic formula for the average number of ideals with a given norm. We do this for arbitrary quadratic orders, and we provide estimates of the remainder term which will be useful in the subsequent section when we investigate the L-functions of quadratic orders.

For a quadratic discriminant Δ with conductor f_Δ, we denote by $\mathcal{J}_\Delta^*$ the set of all non-zero ideals $\mathfrak{a}$ of $\mathcal{O}_\Delta$ such that $(\mathfrak{N}_\Delta(\mathfrak{a}), f_\Delta) = 1$, and for $n \in \mathbb{N}$ we denote by $\mathsf{R}_\Delta(n)$ the number of ideals $\mathfrak{a} \in \mathcal{J}_\Delta^*$ such that $\mathfrak{N}_\Delta(\mathfrak{a}) = n$.

Theorem 8.1.1. *Let Δ be a quadratic discriminant with conductor f_Δ.*

1. *The function $\mathsf{R}_\Delta \colon \mathbb{N} \to \mathbb{N}_0$ is multiplicative,*

$$\mathsf{R}_\Delta(n) = \sum_{d \mid n} \mathsf{Q}_\Delta(d) \quad \textit{for all} \quad n \in \mathbb{N}\,,$$

and if p is a prime and $e \in \mathbb{N}$, then

$$\mathsf{R}_\Delta(p^e) = \begin{cases} e+1 & \textit{if} \quad \mathsf{Q}_\Delta(p) = 1\,, \\ \;\;0 & \textit{if} \quad \mathsf{Q}_\Delta(p) = -1 \;\textit{and}\; e \equiv 1 \mod 2\,, \\ \;\;1 & \textit{otherwise.} \end{cases}$$

2. *We have*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \mathsf{R}_\Delta(n) = \frac{\varphi(f_\Delta)}{f_\Delta}\, L(1, \mathsf{Q}_\Delta)\,.$$

Proof. 1. Let $p \nmid f_\Delta$ be a prime and $\mathfrak{p}_p$ a prime ideal of $\mathcal{O}_\Delta$ containing p. Then Theorem 5.8.8 implies

$$p\mathcal{O}_\Delta = \begin{cases} \mathfrak{p}_p\mathfrak{p}_p' & \text{if} \quad \mathsf{Q}_\Delta(p) = 1\,, \\ \mathfrak{p}_p & \text{if} \quad \mathsf{Q}_\Delta(p) = -1\,, \\ \mathfrak{p}_p^2 & \text{if} \quad \mathsf{Q}_\Delta(p) = 0\,, \end{cases}$$

where $\mathfrak{p}_p$, $\mathfrak{p}_p'$ are prime ideals in $\mathcal{J}_\Delta^*$. By Theorem 5.8.1.4 every ideal $\mathfrak{a} \in \mathcal{J}_\Delta^*$ has a unique factorization

$$\mathfrak{a} = \prod_{\substack{p\in\mathbb{P} \\ \mathsf{Q}_\Delta(p)=1}} \mathfrak{p}_p^{\alpha_p}\mathfrak{p}_p'^{\,\alpha_p'} \prod_{\substack{p\in\mathbb{P} \\ \mathsf{Q}_\Delta(p)=-1}} \mathfrak{p}_p^{\beta_p} \prod_{\substack{p\in\mathbb{P},\, p\nmid f_\Delta \\ \mathsf{Q}_\Delta(p)=0}} \mathfrak{p}_p^{\gamma_p}\,,$$

with exponents α_p, α_p', β_p, $\gamma_p \in \mathbb{N}_0$, and then

$$\mathfrak{N}_\Delta(\mathfrak{a}) = \prod_{\substack{p\in\mathbb{P} \\ \mathsf{Q}_\Delta(p)=1}} p^{\alpha_p+\alpha_p'} \prod_{\substack{p\in\mathbb{P} \\ \mathsf{Q}_\Delta(p)=-1}} p^{2\beta_p} \prod_{\substack{p\in\mathbb{P},\, p\nmid f_\Delta \\ \mathsf{Q}_\Delta(p)=0}} p^{\gamma_p}\,.$$

Consequently, if $n \in \mathbb{N}$ and $\mathsf{v}_p(n) \equiv 0 \mod 2$ for all primes p such that $\mathsf{Q}_\Delta(p) = -1$, then

$$\mathsf{R}_\Delta(n) = \prod_{\substack{p\in\mathbb{P} \\ \mathsf{Q}_\Delta(p)=1}} [\mathsf{v}_p(n) + 1]\,,$$

and $\mathsf{R}_\Delta(n) = 0$ otherwise. Hence R_Δ is a multiplicative function.

For a prime p and $e \in \mathbb{N}$, we obtain

$$\mathsf{R}_\Delta(p^e) = \sum_{\nu=0}^{e} \mathsf{Q}_\Delta(p^\nu) = \begin{cases} e+1 & \text{if} \quad \mathsf{Q}_\Delta(p) = 1\,, \\ 0 & \text{if} \quad \mathsf{Q}_\Delta(p) = -1 \text{ and } e \equiv 1 \mod 2\,, \\ 1 & \text{otherwise.} \end{cases}$$

Since Q_Δ is a multiplicative function, the same is true for its summatory function Q_Δ^*, defined by

$$\mathsf{Q}_\Delta^*(n) = \sum_{1 \le d \,|\, n} \mathsf{Q}_\Delta(d) \quad \text{for all } n \in \mathbb{N}.$$

Since $\mathsf{Q}_\Delta^*(p^e) = \mathsf{R}_\Delta(p^e)$ for all primes p and $e \in \mathbb{N}_0$, it follows that $\mathsf{R}_\Delta = \mathsf{Q}_\Delta^*$.

2. Observe that $\mathsf{Q}_\Delta(n) = \mathsf{R}_\Delta(n) = 0$ if $(n, f_\Delta) \ne 1$. If $N \in \mathbb{N}$, then

$$\sum_{n=1}^{N} \mathsf{R}_\Delta(n) \;=\; \sum_{n=1}^{N} \sum_{1 \le d \,|\, n} \mathsf{Q}_\Delta(d) \;=\; \sum_{\substack{d,\,k=1 \\ dk \le N,\ (k,f_\Delta)=1}}^{\infty} \mathsf{Q}_\Delta(d) \;=\; S_1 + S_2\,,$$

where

$$S_1 = \sum_{1 \le d < \sqrt{N}} \mathsf{Q}_\Delta(d) \sum_{\substack{1 \le k \le \frac{N}{d} \\ (k,f_\Delta)=1}} 1 \qquad \text{and} \qquad S_2 = \sum_{\substack{1 \le k \le \sqrt{N} \\ (k,f_\Delta)=1}} \; \sum_{\sqrt{N} \le d \le \frac{N}{k}} \mathsf{Q}_\Delta(d)\,.$$

Now we obtain

$$S_1 = \sum_{1 \le d < \sqrt{N}} \mathsf{Q}_\Delta(d) \Big[\frac{\varphi(f_\Delta)}{f_\Delta} \frac{N}{d} + \rho_d \Big] = \frac{N \varphi(f_\Delta)}{f_\Delta} \sum_{1 \le d < \sqrt{N}} \frac{\mathsf{Q}_\Delta(d)}{d} + R_N\,,$$

where $\rho_d \in [0, f_\Delta]$ by Lemma A.6.2.4, and

$$R_N = \sum_{1 \le d < \sqrt{N}} \rho_d \in [0, f_\Delta \sqrt{N}\,]\,.$$

Since Q_Δ is a character modulo Δ, Theorem 4.3.1.3 implies

$$|S_2| \le \sum_{1 \le k \le \sqrt{N}} \Big| \sum_{\sqrt{N} \le d \le \frac{N}{d}} \mathsf{Q}_\Delta(d) \Big| \le |\Delta| \sqrt{N}\,.$$

Putting all together, it follows that

$$\Big| \frac{1}{N} \sum_{n=1}^{N} \mathsf{R}_\Delta(n) - \frac{\varphi(f_\Delta)}{f_\Delta} \sum_{1 \le d < \sqrt{N}} \frac{\mathsf{Q}_\Delta(d)}{d} \Big| \le \frac{f_\Delta + |\Delta|}{\sqrt{N}}\,,$$

and therefore

$$\lim_{N \to \infty} \frac{1}{N} \sum_{n=1}^{N} \mathsf{R}_\Delta(n) = \frac{\varphi(f_\Delta)}{f_\Delta} \sum_{n=1}^{\infty} \frac{\mathsf{Q}_\Delta(n)}{n} = \frac{\varphi(f_\Delta)}{f_\Delta} L(1, \mathsf{Q}_\Delta)\,. \qquad \square$$

In the sequel we need a geometric reasoning. Although the following Lemma is obvious from an elementary point of view, we give a formal proof of it. We denote by $\|\cdot\|$ the Euclidean norm of $\mathbb{R}^2$. A subset $C \subset \mathbb{R}^2$ is called a *Lipschitz-bounded curve* if there exist a function $\varphi\colon [0,1] \to \mathbb{R}^2$ and some $L \in \mathbb{R}_{>0}$ such that $C \subset \varphi([0,1])$ and $\|\varphi(t_1) - \varphi(t_2)\| \le L|t_1 - t_2|$ for all $t_1,\ t_2 \in [0,1]$.

Lemma 8.1.2. *Let $\Omega \subset \mathbb{R}^2$ be a set such that its boundary $\partial\Omega$ is a Lipschitz-bounded curve. Let $f \in \mathbb{N}$ be a positive integer and $a,\ b \in \mathbb{Z}$ such that $(a,f) = 1$. For $T \in \mathbb{R}_{>0}$, let*

$$\mathsf{A}_T(f,\Omega) = |\{(x,y) \in T\Omega \cap \mathbb{Z}^2 \mid (ax+by,f) = 1\}|$$

be the number of non-zero lattice points in the expanded domain $T\Omega$ satisfying the side condition $(ax+by,f) = 1$. Then there exists some $M \in \mathbb{R}_{>0}$ such that

$$\Bigl|\frac{\mathsf{A}_T(f,\Omega)}{T^2} - \mu(\Omega)\frac{\varphi(f)}{f}\Bigr| \le \frac{M}{T} \quad \text{for all} \quad T \in \mathbb{R}_{\ge 1}\,,$$

where $\mu(\Omega)$ denotes the (Jordan) content of Ω.

Proof. Let $L \in \mathbb{R}_{>0}$ and $\varphi\colon [0,1] \to \mathbb{R}^2$ be such that $\partial\Omega \subset \varphi([0,1])$ and $\|\varphi(t_1) - \varphi(t_2)\| \le L|t_1 - t_2|$ for all $t_1,\ t_2 \in [0,1]$. By an *integral square* we mean a set of the form $\boldsymbol{a} + [0,1)^2 \subset \mathbb{R}^2$ for some $\boldsymbol{a} \in \mathbb{Z}^2$. We fix some $T \in \mathbb{R}_{>0}$, and we consider first the case $f = 1$. Let $\mathsf{b}_T(\Omega)$ be the number of integral squares contained in $T\Omega$, $\mathsf{B}_T(\Omega)$ the number of integral squares meeting $T\Omega$ and $\mathsf{A}_T(\Omega) = |T\Omega \cap \mathbb{Z}^2|$. Then we obviously have $\mathsf{b}_T(\Omega) \le \mathsf{A}_T(\Omega) \le \mathsf{B}_T(\Omega)$, and the difference $\mathsf{B}_T(\Omega) - \mathsf{b}_T(\Omega)$ is the number of integral squares meeting the boundary $\partial(T\Omega) = T\partial\Omega = T\varphi([0,1])$. Let μ_* denote the inner and μ^* the outer Jordan measure of $\mathbb{R}^2$. Then it follows that $\mu_*(T\Omega) = T^2\mu_*(\Omega)$, $\mu^*(T\Omega) = T^2\mu^*(\Omega)$, and

$$\frac{1}{T^2}\,\mathsf{b}_T(\Omega) \le \mu_*(\Omega) \le \mu^*(\Omega) \le \frac{1}{T^2}\,\mathsf{B}_T(\Omega)\,.$$

We set

$$k = \Bigl\lceil \frac{TL}{\sqrt{2}} \Bigr\rceil, \quad \text{and we consider an interval} \quad I_j = \Bigl[\frac{j}{k}, \frac{j+1}{k}\Bigr] \quad \text{for some} \quad j \in [0, k-1]\,.$$

Suppose that $t_0 \in I_j$ and $T\varphi(t_0) \in (x_0,y_0) + [0,1)^2$ for some $(x_0,y_0) \in \mathbb{Z}^2$. Then the square $Q = (x_0-1, y_0-1) + [0,3)^2$ is the union of nine integral squares, and $\{\boldsymbol{z} \in \mathbb{R}^2 \mid \|\boldsymbol{z} - T\varphi(t_0)\| \le \sqrt{2}\,\} \subset Q$. If $t \in I_j$, then

$$|t - t_0| \le \frac{1}{k}, \quad \text{hence} \quad \|T\varphi(t) - T\varphi(t_0)\| \le \frac{TL}{k} \le \sqrt{2}\,, \quad \text{and therefore} \quad T\varphi(t) \in Q\,.$$

Hence $\partial(T\Omega)$ is contained in the union of at most $9k$ integral squares, and we obtain

$$\mu^*(\Omega) - \mu_*(\Omega) \le \frac{1}{T^2}\bigl[\,\mathsf{B}_T(\Omega) - \mathsf{b}_T(\Omega)\,\bigr] \le \frac{9k}{T^2} \le \frac{9L}{T\sqrt{2}} + \frac{9}{T^2}\,.$$

For $T \to \infty$, it follows that $\mu_*(\Omega) = \mu^*(\Omega)$, hence Ω is Jordan measurable. Moreover, there exists some $M_1 \in \mathbb{R}_{>0}$ such that

$$\Bigl|\mu(\Omega) - \frac{\mathsf{A}_T(\Omega)}{T^2}\Bigr| \le \frac{1}{T^2}\bigl[\,\mathsf{B}_T(\Omega) - \mathsf{b}_T(\Omega)\,\bigr] \le \frac{M_1}{T} \quad \text{for all} \quad T \in \mathbb{R}_{\ge 1}\,.$$

If Q is an integral square, then we call the expanded square fQ an *f-square*, we obviously have $|fQ \cap \mathbb{Z}^2| = f^2$, and we assert that

$$(*) \qquad |\{(x,y) \in fQ \cap \mathbb{Z}^2 \mid (ax+by, f) = 1\}| = f\varphi(f)\,.$$

Assume that $(*)$ holds. Since $\mathsf{b}_T(\Omega)$ is the number of f-squares contained in $Tf\Omega$ and $\mathsf{B}_T(\Omega)$ is the number of f-squares meeting $Tf\Omega$, $(*)$ implies that

$$f^2\mathsf{b}_T(\Omega) \le \mathsf{A}_{Tf}(\Omega) \le f^2\mathsf{B}_T(\Omega) \quad \text{and} \quad f\varphi(f)\mathsf{b}_T(\Omega) \le \mathsf{A}_{Tf}(f,\Omega) \le f\varphi(f)\mathsf{B}_T(\Omega)\,.$$

Combining these two inequalities, it follows that

$$\Bigl|\frac{\varphi(f)}{f}\,\frac{\mathsf{A}_{Tf}(\Omega)}{(Tf)^2} - \frac{\mathsf{A}_{Tf}(f,\Omega)}{(Tf)^2}\Bigr| \le \frac{\varphi(f)}{fT^2}[\mathsf{B}_T(\Omega) - \mathsf{b}_T(\Omega)] \le \frac{\varphi(f)}{f}\,\frac{M_1}{T} \quad \text{for all } \ T \in \mathbb{R}_{\ge 1}\,.$$

We replace Tf by T and obtain, now for all $T \ge f$,

$$\Bigl|\frac{\varphi(f)}{f}\,\frac{\mathsf{A}_T(\Omega)}{T^2} - \frac{\mathsf{A}_T(f,\Omega)}{T^2}\Bigr| \le \frac{\varphi(f)M_1}{T}\,.$$

Hence it follows that

$$\Bigl|\frac{\mathsf{A}_T(f,\Omega)}{T^2} - \mu(\Omega)\frac{\varphi(f)}{f}\Bigr| \le \frac{\varphi(f)}{f}\Bigl|\frac{\mathsf{A}_T(\Omega)}{T^2} - \mu(\Omega)\Bigr| + \Bigl|\frac{\varphi(f)}{f}\,\frac{\mathsf{A}_T(\Omega)}{T^2} - \frac{\mathsf{A}_T(f,\Omega)}{T^2}\Bigr| \le \frac{M}{T}$$

for some constant $M \in \mathbb{R}_{>0}$ and all $T \in \mathbb{R}_{\ge 1}$.

Proof of $(*)$. If Q is any integral square, then

$$\bigl|\{(x,y) \in fQ \cap \mathbb{Z}^2 \mid (ax+by,f) = 1\}\bigr| = \bigl|\{(x,y) \in [0,f-1]^2 \bigm| (ax+by,f) = 1\}\bigr|\,.$$

For every $y \in [0, f-1]$, we consider the map $\varphi_y\colon [0,f-1] \to \mathbb{Z}/f\mathbb{Z}$, defined by $\varphi_y(x) = ax+by+f\mathbb{Z}$. Since $(a,f) = 1$, φ_y is bijective, and if $(x,y) \in [0,f-1]^2$, then $(ax+by,f) = 1$ if and only if $ax+by+f\mathbb{Z} \in (\mathbb{Z}/f\mathbb{Z})^\times$. Hence it follows that

$$|\{(x,y) \in [0,f-1]^2 \mid (ax+by,f) = 1\}| = f\varphi(f)\,. \qquad \square$$

Theorem 8.1.3. *Let Δ be a quadratic discriminant with conductor f_Δ.*

- *If $\Delta < 0$, we set*

$$\lambda_\Delta = \frac{2\pi}{\mathsf{w}_\Delta\sqrt{|\Delta|}}\,, \quad \textit{where} \ \ \mathsf{w}_\Delta = |\mathcal{O}_\Delta^\times| = \begin{cases} 6 & \textit{if} \ \ \Delta = -3\,, \\ 4 & \textit{if} \ \ \Delta = -4\,, \\ 2 & \textit{if} \ \ \Delta < -4\,. \end{cases}$$

- *If $\Delta > 0$, we set*

$$\lambda_\Delta = \frac{\log \varepsilon_\Delta^+}{\sqrt{\Delta}}\,,$$

  where ε_Δ^+ denotes the norm-positive fundamental unit of discriminant Δ.

Let $C \in \mathcal{C}_\Delta^+$ be a narrow ideal class. For $N \in \mathbb{N}$, let $\mathsf{R}_C^*(N)$ be the number of ideals $\mathfrak{a} \in \mathcal{I}_\Delta^*$ lying in C such that $\mathfrak{N}_\Delta(\mathfrak{a}) \le N$. Then there exists some $B \in \mathbb{R}_{>0}$ such that

$$\Bigl|\frac{1}{N}\,\mathsf{R}_C^*(N) - \lambda_\Delta\frac{\varphi(f_\Delta)}{f_\Delta}\Bigr| \le \frac{B}{\sqrt{N}} \quad \textit{for all} \quad N \in \mathbb{N}\,,$$

and consequently

$$\lim_{N\to\infty} \frac{1}{N}\,\mathsf{R}_C^*(N) = \lambda_\Delta\frac{\varphi(f_\Delta)}{f_\Delta}\,.$$

PROOF. We fix an $\mathcal{O}_\Delta$-regular ideal $\mathfrak{a}_1 \in C^{-1}$ such that $(\mathfrak{N}_\Delta(\mathfrak{a}_1), f_\Delta) = 1$ (see Theorem 5.5.7.2(b)). For $N \in \mathbb{N}$, we assert that

$$(*) \qquad \mathsf{R}^*_C(N) = |\{\alpha\mathcal{O}_\Delta \mid \alpha \in \mathfrak{a}_1,\ (\mathcal{N}(\alpha), f_\Delta) = 1,\ 0 < \mathcal{N}(\alpha) \le N\mathfrak{N}_\Delta(\mathfrak{a}_1)\}|\,.$$

Indeed, if $N \in \mathbb{N}$, $\alpha \in \mathfrak{a}_1$, $(\mathcal{N}(\alpha), f_\Delta) = 1$ and $0 < \mathcal{N}(\alpha) \le N\mathfrak{N}_\Delta(\mathfrak{a}_1)$, then $\alpha\mathfrak{a}_1^{-1}$ is a non-zero ideal of $\mathcal{O}_\Delta$ lying in C, and since $\mathfrak{N}_\Delta(\alpha\mathfrak{a}_1^{-1})\mathfrak{N}_\Delta(\mathfrak{a}_1) = \mathcal{N}(\alpha)$, it follows that

$$(\mathfrak{N}_\Delta(\alpha\mathfrak{a}_1^{-1}), f_\Delta) = 1 \quad \text{and} \quad \mathfrak{N}_\Delta(\alpha\mathfrak{a}_1^{-1}) = \frac{\mathcal{N}(\alpha)}{\mathfrak{N}_\Delta(\mathfrak{a}_1)} \le N\,.$$

Conversely, if $\mathfrak{a} \in \mathcal{J}^*_\Delta$ is an ideal in C such that $\mathfrak{N}_\Delta(\mathfrak{a}) \le N$, then $\mathfrak{a}\mathfrak{a}_1 = \alpha\mathcal{O}_\Delta$ for some $\alpha \in \mathfrak{a}_1$ satisfying $0 < \mathcal{N}(\alpha) = \mathfrak{N}_\Delta(\mathfrak{a})\mathfrak{N}_\Delta(\mathfrak{a}_1) \le N\mathsf{N}_\Delta(\mathfrak{a}_1)$ and $(\mathcal{N}(\alpha), f_\Delta) = 1$. Since the principal ideal $\alpha\mathcal{O}_\Delta$ is uniquely determined by $\mathfrak{a}$, this proves $(*)$.

By Theorem 5.4.2.1, the ideal $\mathfrak{a}_1$ is of the form

$$\mathfrak{a}_1 = \mathbb{Z}a + \mathbb{Z}\,\frac{b+\sqrt{\Delta}}{2}\,, \quad \text{where} \quad a = \mathfrak{N}_\Delta(\mathfrak{a}_1)\,,\ b,\, c \in \mathbb{Z} \ \text{ and } \ \Delta = b^2 - 4ac\,.$$

If $\alpha \in \mathfrak{a}_1$, then there exist $x,\, y \in \mathbb{Z}$ such that

$$\alpha = ax + \frac{b+\sqrt{\Delta}}{2}y\,,$$

and then

$$\mathcal{N}(\alpha) = \Bigl(ax + \frac{by}{2}\Bigr)^2 - \frac{\Delta y^2}{4} = (ax^2 + bxy + cy^2)\mathfrak{N}_\Delta(\mathfrak{a}_1)\,.$$

Now we analyze the condition $(\mathcal{N}(\alpha), f_\Delta) = 1$. If $\Delta \equiv 0 \bmod 4$, we set $b = 2b^*$ and $a = a^*$. If $\Delta \equiv 1 \bmod 4$, we set $b^* = b$ and $a^* = 2a$. Then it is obvious that $a^*, b^* \in \mathbb{Z}$, $(a^*, f_\Delta) = 1$, and if $(x, y) \in \mathbb{Z}^2$, then $(ax^2 + bxy + cy^2, f_\Delta) = 1$ holds if and only if $(a^*x + b^*y, f_\Delta) = 1$.

CASE 1: $\Delta < 0$. If $\alpha,\, \alpha_1 \in \mathcal{O}^\bullet_\Delta$, then $\alpha\mathcal{O}_\Delta = \alpha_1\mathcal{O}_\Delta$ if and only if $\alpha_1 = \alpha\varepsilon$ for some $\varepsilon \in \mathcal{O}^\times_\Delta$, and therefore

$$\begin{aligned}\mathsf{w}_\Delta\mathsf{R}^*_C(N) &= |\{\alpha \in \mathfrak{a}_1 \mid (\mathcal{N}(\alpha), f_\Delta) = 1,\ 0 < \mathcal{N}(\alpha) \le N\mathfrak{N}_\Delta(\mathfrak{a}_1)\}| \\ &= |\{(x,y) \in \mathbb{Z}^2 \mid (a^*x + b^*y, f_\Delta) = 1\,,\ 0 < ax^2 + bxy + cy^2 \le N\}| \\ &= |\{(x,y) \in \mathbb{Z}^2 \cap \sqrt{N}\mathcal{E} \mid (a^*x + b^*y, f_\Delta) = 1\,,\ (x,y) \ne (0,0)\}|\,,\end{aligned}$$

where

$$\mathcal{E} = \{(x,y) \in \mathbb{R}^2 \mid ax^2 + bxy + cy^2 \le 1\} = \Bigl\{(x,y) \in \mathbb{R}^2 \Bigm| \frac{1}{a}\Bigl(ax + \frac{b}{2}y\Bigr)^2 + \frac{|\Delta|}{4a}y^2 \le 1\Bigr\}$$

is an ellipse having the semi-axes

$$\frac{1}{\sqrt{a}} \quad \text{and} \quad \frac{2\sqrt{a}}{\sqrt{|\Delta|}}\,, \quad \text{and therefore} \quad \mu(\mathcal{E}) = \frac{2\pi}{\sqrt{|\Delta|}} = \mathsf{w}_\Delta\lambda_\Delta\,.$$

Now we apply Lemma 8.1.2 and take care of the condition $(x,y) \ne (0,0)$. Since $\mathsf{w}_\Delta\mathsf{R}^*_C(N) = \mathsf{A}_{\sqrt{N}}(f, \mathcal{E}) - e$, where $e \in \{0,1\}$, there exists some constant $B_1 \in \mathbb{R}_{>0}$ such that

$$\Bigl|\frac{\mathsf{w}_\Delta\mathsf{R}^*_C(N)}{N} - \mu(\mathcal{E})\frac{\varphi(f_\Delta)}{f_\Delta}\Bigr| \le \frac{B_1}{\sqrt{N}}\,, \quad \text{and therefore} \quad \Bigl|\frac{\mathsf{R}^*_C(N)}{N} - \lambda_\Delta\frac{\varphi(f_\Delta)}{f_\Delta}\Bigr| \le \frac{B_1}{\mathsf{w}_\Delta\sqrt{N}}\,.$$

CASE 2: $\Delta > 0$. For $N \in \mathbb{N}$, Theorem 5.2.5.3 implies that $\mathsf{R}^*_C(N)$ is the number of elements $\alpha \in \mathfrak{a}_1$ satisfying the conditions

$$\alpha > 0\,, \quad (\mathcal{N}(\alpha), f_\Delta) = 1\,, \quad 0 < \mathcal{N}(\alpha) \le N\mathfrak{N}_\Delta(\mathfrak{a}_1) \quad \text{and} \quad 1 < \frac{\alpha'}{\alpha} \le \varepsilon_\Delta^{+2}\,.$$

We set

$$\theta = \frac{b + \sqrt{\Delta}}{2a}\,.$$

Then every $\alpha \in \mathfrak{a}_1$ has a unique representation in the form $\alpha = a(x + \theta y)$ for some $x, y \in \mathbb{Z}$. If α is given in this way, then $\mathcal{N}(\alpha) = a^2(x + \theta y)(x + \theta' y)$ and $(\mathcal{N}(\alpha), f_\Delta) = 1$ if and only if $(a^* x + b^* y, f_\Delta) = 1$. Hence we obtain

$$\mathsf{R}^*_C(N) = \bigl|\bigl\{(x, y) \in \mathbb{Z}^2 \cap \sqrt{N}\mathcal{H} \bigm| (a^* x + b^* y, f_\Delta) = 1\,,\ (x, y) \ne (0, 0)\bigr\}\bigr|\,,$$

where

$$\mathcal{H} = \Bigl\{(x, y) \in \mathbb{R}^2 \Bigm| x + \theta y > 0,\ 0 < a(x + \theta y)(x + \theta' y) \le 1,\ 1 < \frac{x + \theta' y}{x + \theta y} \le \varepsilon_\Delta^{+2}\Bigr\}\,.$$

We apply Lemma 8.1.2 and take care of the condition $(x, y) \ne (0, 0)$. We obtain $\mathsf{R}^*_C(N) = \mathsf{A}_{\sqrt{N}}(f, \mathcal{H}) - e$, where $e \in \{0, 1\}$, and therefore there exists some constant $B \in \mathbb{R}_{>0}$ such that

$$\Bigl|\frac{\mathsf{R}^*_C(N)}{N} - \mu(\mathcal{H})\frac{\varphi(f_\Delta)}{f_\Delta}\Bigr| \le \frac{B}{\sqrt{N}}\,.$$

In order to calculate $\mu(\mathcal{H})$, we make the substitution

$$\xi = (x + \theta y)\sqrt{a}\,, \quad \eta = (x + \theta' y)\sqrt{a}$$

with the Jacobian

$$\det\begin{pmatrix} \frac{\partial \xi}{\partial x} & \frac{\partial \xi}{\partial y} \\ \frac{\partial \eta}{\partial x} & \frac{\partial \eta}{\partial y} \end{pmatrix} = \det\begin{pmatrix} \sqrt{a} & \theta\sqrt{a} \\ \sqrt{a} & \theta'\sqrt{a} \end{pmatrix} = (\theta' - \theta)a = -\sqrt{\Delta}\,,$$

and we obtain

$$\mu(\mathcal{H}) = \frac{\mu(\mathcal{H}^*)}{\sqrt{\Delta}}\,, \quad \text{where } \mathcal{H}^* = \{(\xi, \eta) \in \mathbb{R}^2 \bigm| \xi > 0, \ \ 0 < \xi\eta \le 1, \ \ \xi < \eta \le \varepsilon_\Delta^{+2}\xi\}\,.$$

If $(\xi, \eta) \in \mathcal{H}^*$, then $0 < \eta \le \varepsilon_\Delta^{+2}\xi \le \varepsilon_\Delta^{+2}\eta^{-1}$, hence $0 < \eta \le \varepsilon_\Delta^+$, and we obtain

$$\begin{aligned}
\mathcal{H}^* &= \Bigl\{(\xi, \eta) \in \mathbb{R}^2 \Bigm| 0 < \eta \le \varepsilon_\Delta^+,\ \ \frac{\eta}{\varepsilon^{+2}} \le \xi \le \min\Bigl(\frac{1}{\eta}, \eta\Bigr)\Bigr\} \\
&= \Bigl\{(\xi, \eta) \in \mathbb{R}^2 \Bigm| 0 < \eta \le 1,\ \ \frac{\eta}{\varepsilon_\Delta^{+2}} < \xi \le \eta\Bigr\} \\
&\qquad \uplus \Bigl\{(\xi, \eta) \in \mathbb{R}^2 \Bigm| 1 < \eta \le \varepsilon_\Delta^+,\ \ \frac{\eta}{\varepsilon_\Delta^{+2}} < \xi \le \frac{1}{\eta}\Bigr\}\,.
\end{aligned}$$

Now it is easy to calculate the volume:

$$\begin{aligned}\mu(\mathcal{H}^*) &= \int_0^1 d\eta \int_{\eta/\varepsilon_\Delta^{+2}}^{\eta} d\xi \;+\; \int_1^{\varepsilon_\Delta^+} d\eta \int_{\eta/\varepsilon_\Delta^{+2}}^{1/\eta} d\xi \\ &= \int_0^1 \Big(\eta - \frac{\eta}{\varepsilon_\Delta^{+2}}\Big) d\eta \;+\; \int_1^{\varepsilon_\Delta^+} \Big(\frac{1}{\eta} - \frac{\eta}{\varepsilon_\Delta^{+2}}\Big) d\eta \\ &= \frac{1}{2}\Big(1 - \frac{1}{\varepsilon_\Delta^{+2}}\Big) + \log\varepsilon_\Delta^+ - \frac{1}{\varepsilon_\Delta^{+2}}\Big(\frac{\varepsilon_\Delta^{+2}}{2} - \frac{1}{2}\Big) = \log\varepsilon_\Delta^+ .\end{aligned}$$

Thus we finally obtain $\mu(\mathcal{H}) = \lambda_\Delta$, and the assertion follows. □

Theorem 8.1.4. *Let Δ be a quadratic discriminant.*

- *If $\Delta < 0$, then*

$$h_\Delta = \frac{\mathsf{w}_\Delta\sqrt{|\Delta|}}{2\pi}\, L(1,\mathsf{Q}_\Delta)\,, \quad \textit{where} \quad \mathsf{w}_\Delta = |\mathcal{O}_\Delta^\times| = \begin{cases} 6 & \textit{if} \quad \Delta = -3\,, \\ 4 & \textit{if} \quad \Delta = -4\,, \\ 2 & \textit{if} \quad \Delta < -4\,, \end{cases}$$

- *If $\Delta > 0$, then*

$$h_\Delta^+ = \frac{\sqrt{\Delta}}{\log\varepsilon_\Delta^+}\, L(1,\mathsf{Q}_\Delta) \quad \textit{and} \quad h_\Delta = \frac{\sqrt{\Delta}}{2\log\varepsilon_\Delta}\, L(1,\mathsf{Q}_\Delta)\,.$$

Proof. Let f_Δ be the conductor of Δ and λ_Δ as in Theorem 8.1.3. By the Theorems 8.1.1 and 8.1.3 we obtain

$$\frac{\varphi(f_\Delta)}{f_\Delta}\, L(1,\mathsf{Q}_\Delta) = \lim_{N\to\infty}\frac{1}{N}\sum_{n=1}^{N}\mathsf{R}_\Delta(n) = \lim_{N\to\infty}\frac{1}{N}\sum_{C\in\mathcal{C}_\Delta^+}\mathsf{R}_C^*(N) = \lambda_\Delta\,\frac{\varphi(f_\Delta)}{f_\Delta}\,|\mathcal{C}_\Delta^+|\,,$$

and therefore

$$|\mathcal{C}_\Delta^+| = \frac{1}{\lambda_\Delta}\, L(1,\mathsf{Q}_\Delta)\,.$$

If $\Delta < 0$, then $h_\Delta = |\mathcal{C}_\Delta| = |\mathcal{C}_\Delta^+|$. If $\Delta > 0$, then $h_\Delta^+ = |\mathcal{C}_\Delta^+|$, and the connection of h_Δ and h_Δ^+ was given in Theorem 5.5.4. If $\mathcal{N}(\varepsilon_\Delta) = 1$, then $\varepsilon_\Delta = \varepsilon_\Delta^+$ and $h_\Delta^+ = 2h_\Delta$. If $\mathcal{N}(\varepsilon_\Delta) = -1$, then $\varepsilon_\Delta^2 = \varepsilon_\Delta^+$ and $h_\Delta^+ = h_\Delta$. In both cases, we obtain the asserted formula for h_Δ. □

Exercise 8.1.5. Let $\Delta = \Delta_0 f_\Delta^2$ be a quadratic discriminant with fundamental discriminant Δ_0 and conductor f_Δ. Prove that

$$L(1,\mathsf{Q}_\Delta) = L(1,\mathsf{Q}_{\Delta_0}\prod_{p\,|\,f_\Delta}\Big(1 - \frac{\mathsf{Q}_\Delta(p)}{p}\Big)\,.$$

Use Theorem 8.1.4 to deduce the formula

$$\frac{h_\Delta}{h_{\Delta_0}} = \frac{f_\Delta}{(\mathcal{O}_{\Delta_0}^\times : \mathcal{O}_\Delta^\times}\prod_{p\,|\,f_\Delta}\Big(1 - \frac{\mathsf{Q}_\Delta(p)}{p}\Big)\,.$$

(In Theorem, 5.9.7.4 we gave a structural algebraic proof of this formula.)

Now we restrict to the case of a fundamental discriminant Δ. Then the quadratic character Q_Δ is primitive by Theorem 3.5.6, and we know the value of the Gauss sums $\tau(\mathsf{Q}_\Delta)$ by Theorem 3.5.8.

Theorem 8.1.6. *Let Δ be a fundamental discriminant.*

1. *Suppose that $\Delta < 0$. Then*

$$h_\Delta = -\frac{\mathsf{w}_\Delta}{2|\Delta|} \sum_{j=1}^{|\Delta|-1} \mathsf{Q}_\Delta(j)j\,, \quad \textit{where} \quad \mathsf{w}_\Delta = \begin{cases} 6 & \textit{if} \quad \Delta = -3\,, \\ 4 & \textit{if} \quad \Delta = -4\,, \\ 2 & \textit{if} \quad \Delta < -4\,, \end{cases}$$

and if $\Delta < -4$, then

$$h_\Delta = \frac{1}{2 - \mathsf{Q}_\Delta(2)} \sum_{1 \le j < \frac{|\Delta|}{2}} \mathsf{Q}_\Delta(j)\,.$$

2. *If $\Delta > 0$, then*

$$h_\Delta = \frac{-1}{\log \varepsilon_\Delta} \sum_{1 \le j < \frac{\Delta}{2}} \mathsf{Q}_\Delta(j) \log \sin \frac{\pi j}{\Delta}\,, \quad \textit{and} \quad \varepsilon_\Delta^{h_\Delta} = \prod_{1 \le j < \frac{\Delta}{2}} \Big(\sin \frac{\pi j}{\Delta}\Big)^{-\mathsf{Q}_\Delta(j)}\,.$$

PROOF. 1. We have $\mathsf{Q}_\Delta(-1) = -1$ by Theorem 3.5.5.1, $\tau(\mathsf{Q}_\Delta) = \sqrt{\Delta} = \mathsf{i}\sqrt{|\Delta|}$ and

$$L(1, \mathsf{Q}_\Delta) = \frac{\mathsf{i}\pi\tau(\mathsf{Q}_\Delta)}{|\Delta|^2} \sum_{j=1}^{|\Delta|-1} \mathsf{Q}_\Delta(j)j = \frac{-\pi}{|\Delta|^{3/2}} \sum_{j=1}^{|\Delta|-1} \mathsf{Q}_\Delta(j)j$$

by Theorem 4.4.2. Thus we obtain (by Theorem 8.1.4)

$$h_\Delta = \frac{\mathsf{w}_\Delta\sqrt{|\Delta|}}{2\pi} L(1, \mathsf{Q}_\Delta) = \frac{-\mathsf{w}_\Delta}{2|\Delta|} \sum_{j=1}^{|\Delta|-1} \mathsf{Q}_\Delta(j)j\,.$$

Assume now that $\Delta < -4$. Then $\mathsf{w}_\Delta = 2$, and

$$h_\Delta = -\frac{1}{|\Delta|} \sum_{j=1}^{|\Delta|-1} \mathsf{Q}_\Delta(j)j\,.$$

CASE 1: $\Delta \equiv 0 \bmod 4$. The $\mathsf{Q}_\Delta(2) = 0$, we set $|\Delta| = 2m$, and observe that $\mathsf{Q}_\Delta(a+m) = -\mathsf{Q}_\Delta(a)$ for all $a \in \mathbb{Z}$ (see Theorem 3.5.5.2(b)). Hence

$$\sum_{j=1}^{|\Delta|-1} \mathsf{Q}_\Delta(j)j = \sum_{j=1}^{m-1} \mathsf{Q}_\Delta(j)j + \sum_{j=1}^{m-1} \mathsf{Q}_\Delta(m+j)(m+j)$$

$$= \sum_{j=1}^{m-1} \mathsf{Q}_\Delta(j)j - \sum_{j=1}^{m-1} \mathsf{Q}_\Delta(j)(m+j) = -m \sum_{j=1}^{m-1} \mathsf{Q}_\Delta(j) = -\frac{|\Delta|}{2} \sum_{1 \le j < \frac{|\Delta|}{2}} \mathsf{Q}_\Delta(j)\,,$$

and the assertion follows.

CASE 2: $\Delta \equiv 1 \bmod 4$. We set $|\Delta| = 2m+1$ and obtain

$$\sum_{j=1}^{|\Delta|-1} \mathsf{Q}_\Delta(j)j = \sum_{j=1}^{2m} \mathsf{Q}_\Delta(j)j = \sum_{j=1}^{m} \mathsf{Q}_\Delta(j)j + \sum_{j=1}^{m} \mathsf{Q}_\Delta(|\Delta|-j)(|\Delta|-j)$$
$$= 2\sum_{j=1}^{m} \mathsf{Q}_\Delta(j)j - |\Delta|\sum_{j=1}^{m} \mathsf{Q}_\Delta(j)\,.$$

On the other hand,

$$\sum_{j=1}^{2m} \mathsf{Q}_\Delta(j)j = \sum_{j=1}^{m} \mathsf{Q}_\Delta(2j)(2j) + \sum_{j=1}^{m} \mathsf{Q}_\Delta(|\Delta|-2j)(|\Delta|-2j)$$
$$= 2\mathsf{Q}_\Delta(2)\sum_{j=1}^{m} \mathsf{Q}_\Delta(j)j - |\Delta|\mathsf{Q}_\Delta(2)\sum_{j=1}^{m} \mathsf{Q}_\Delta(j) + 2\mathsf{Q}_\Delta(2)\sum_{j=1}^{m} \mathsf{Q}_\Delta(j)j$$
$$= 4\mathsf{Q}_\Delta(2)\sum_{j=1}^{m} \mathsf{Q}_\Delta(j)j - |\Delta|\mathsf{Q}_\Delta(2)\sum_{j=1}^{m} \mathsf{Q}_\Delta(j)\,.$$

Combining these two expressions, we find

$$(2-\mathsf{Q}_\Delta(2))\sum_{j=1}^{2m} \mathsf{Q}_\Delta(j)j = \ 4\sum_{j=1}^{m} \mathsf{Q}_\Delta(j)j - 2|\Delta|\sum_{j=1}^{m} \mathsf{Q}_\Delta(j)$$
$$-4\sum_{j=1}^{m} \mathsf{Q}_\Delta(j)j + |\Delta|\sum_{j=1}^{m} \mathsf{Q}_\Delta(j) = -|\Delta|\sum_{j=1}^{m} \mathsf{Q}_\Delta(j)\,,$$

and therefore

$$\sum_{j=1}^{2m} \mathsf{Q}_\Delta(j)j = -\frac{|\Delta|}{2-\mathsf{Q}_\Delta(2)}\sum_{1\le j<\frac{|\Delta|}{2}} \mathsf{Q}_\Delta(j)\,,$$

which implies our assertion.

2. Suppose that $\Delta > 0$. Then $\tau(\mathsf{Q}_\Delta) = \sqrt{\Delta}$, hence

$$L(1,\mathsf{Q}_\Delta) = \frac{-1}{\sqrt{\Delta}}\sum_{j=1}^{\Delta-1} \mathsf{Q}_\Delta(j)\log\sin\frac{\pi j}{\Delta}$$

by Theorem 4.4.2, and by Theorem 8.1.4 we obtain

$$h_\Delta = \frac{\sqrt{\Delta}}{2\log\varepsilon_\Delta}L(1,\mathsf{Q}_\Delta) = \frac{-1}{2\log\varepsilon_\Delta}\sum_{j=1}^{\Delta-1} \mathsf{Q}_\Delta(j)\log\sin\frac{\pi j}{\Delta}\,.$$

Since

$$\sum_{j=1}^{\Delta-1} \mathsf{Q}_\Delta(j)\log\sin\frac{\pi j}{\Delta} = \sum_{1\le j<\frac{\Delta}{2}} \mathsf{Q}_\Delta(j)\log\sin\frac{\pi j}{\Delta} + \sum_{1\le j<\frac{\Delta}{2}} \mathsf{Q}_\Delta(\Delta-j)\log\sin\frac{\pi(\Delta-j)}{\Delta}$$
$$= 2\sum_{1\le j<\frac{\Delta}{2}} \mathsf{Q}_\Delta(j)\log\sin\frac{\pi j}{\Delta}\,,$$

we obtain

$$h_\Delta = \frac{-1}{\log \varepsilon_\Delta} \sum_{1 \le j < \frac{\Delta}{2}} \mathsf{Q}_\Delta(j) \log \sin \frac{\pi j}{\Delta} \;=\; \frac{1}{\log \varepsilon_\Delta} \log \prod_{1 \le j < \frac{\Delta}{2}} \Bigl(\sin \frac{\pi j}{\Delta}\Bigr)^{-\mathsf{Q}_\Delta(j)}$$

and finally

$$\varepsilon_\Delta^{h_\Delta} = \prod_{1 \le j < \frac{\Delta}{2}} \Bigl(\sin \frac{\pi j}{\Delta}\Bigr)^{-\mathsf{Q}_\Delta(j)}. \qquad \square$$

Exercise 8.1.7. Use Theorem 8.1.6 to calculate h_{-3}, h_{-23}, h_8 and h_{12}.

Exercise 8.1.8. Let $\Delta > 0$ be a quadratic discriminant. Prove that

$$\varepsilon_\Delta^{2h_\Delta} \prod_{\substack{j=1 \\ \mathsf{Q}_\Delta(j)=1}}^{\Delta-1} |1 - \zeta_\Delta^j| = \prod_{\substack{j=1 \\ \mathsf{Q}_\Delta(j)=-1}}^{\Delta-1} |1 - \zeta_\Delta^j|\,.$$

Theorem 8.1.9. *Let* $p \equiv 3 \bmod 4$ *be a prime,* $p \ne 3$. *Let* R *denote the number of quadratic residues and* N *the number of quadratic non-residues modulo* p *in the interval* $[0, (p-1)/2\,]$. *Then*

$$h_{-p} = \frac{1}{q}\,(R - N)\,, \quad \textit{where} \quad q = \begin{cases} 1 & \textit{if} \;\; p \equiv 7 \bmod 8\,, \\ 3 & \textit{if} \;\; p \equiv 3 \bmod 8\,. \end{cases}$$

Proof. By Theorem 8.1.6 we obtain (using Theorem 3.5.4)

$$h_{-p} = \frac{1}{2 - \mathsf{Q}_{-p}(a)} \sum_{j=1}^{(p-1)/2} \mathsf{Q}_{-p}(j) = \frac{1}{2 - \bigl(\frac{2}{p}\bigr)} \Biggl[\sum_{\substack{j=1 \\ (\frac{j}{p})=1}}^{(p-1)/2} 1 \;-\; \sum_{\substack{j=1 \\ (\frac{j}{p})=-1}}^{(p-1)/2} 1\Biggr]$$

$$= \frac{1}{q}(R - N)\,. \qquad \square$$

Let $p \equiv 3 \bmod 4$ be a prime. We know that

$$\Bigl(\frac{p-1}{2}\Bigr)! \equiv \pm 1 \mod p$$

(see Theorem A.6.3.5). Now we are able to determine the sign.

Corollary 8.1.10. *Let* $p \equiv 3 \bmod 4$ *be a prime. Then*

$$\Bigl(\frac{p-1}{2}\Bigr)! \equiv 1 \bmod p \quad \textit{if and only if} \quad h_{-p} \equiv -1 \bmod 4\,.$$

Proof. Let R denote the number of quadratic residues and N the number of quadratic non-residues modulo p in the interval $[0, (p-1)/2\,]$. Let $\varepsilon_p \in \{\pm 1\}$ be such that

$$\Bigl(\frac{p-1}{2}\Bigr)! \equiv \varepsilon_p \mod p\,, \quad \text{and observe that} \quad \Bigl(\frac{p-1}{2}\Bigr)! \equiv (-1)^N \mod 4\,.$$

It follows that $\varepsilon_p = (-1)^N$. By Theorem 8.1.9 we have

$$h_{-p} = \frac{1}{q}(R-N) = \frac{1}{q}\Big(\frac{p-1}{2} - 2N\Big)\,, \quad \text{where} \quad q = \begin{cases} 1 & \text{if} \quad p \equiv 7 \bmod 8\,, \\ 3 & \text{if} \quad p \equiv 3 \bmod 8\,. \end{cases}$$

In both cases, it follows that $h_{-p} \equiv 3 - 2N \bmod 4$, and thus $N \equiv 0 \bmod 2$ if and only if $h_{-p} \equiv -1 \bmod 4$. □

8.2. *L*-functions of quadratic orders

In this section, we introduce the L-functions of a quadratic order attached with characters of its narrow ideal class group. By the way, we obtain a fresh interpretation of the analytic class number formula and a generalization of Dirichlet's prime number theorem to quadratic orders. In particular, we shall prove that every primitive form represents infinitely many primes.

For a quadratic discriminant Δ with conductor f_Δ, let (as before) $\mathcal{J}_\Delta^*$ be the set of all non-zero ideals $\mathfrak{a}$ of $\mathcal{O}_\Delta$ such that $(\mathfrak{N}_\Delta(\mathfrak{a}), f_\Delta) = 1$ and $\mathcal{P}_\Delta$ the set of all prime ideals in $\mathcal{J}_\Delta^*$.

We consider the character group $\mathfrak{C}_\Delta = \widehat{\mathcal{C}_\Delta^+} = \mathrm{Hom}(\mathcal{C}_\Delta^+, \mathbb{C}^\times)$. Its elements are called *ideal class characters* of $\mathcal{O}_\Delta$. We denote by $\mathbf{1} \in \mathfrak{C}_\Delta$ the unit character. For $\phi \in \mathfrak{C}_\Delta$ and $\mathfrak{a} \in \mathcal{J}_\Delta^*$, we set $\phi(\mathfrak{a}) = \phi([\mathfrak{a}]^+)$, and for $n \in \mathbb{N}$, we set

$$\phi^*(n) = \sum_{\substack{\mathfrak{a} \in \mathcal{J}_\Delta^* \\ \mathfrak{N}_\Delta(\mathfrak{a}) = n}} \phi(\mathfrak{a})\,.$$

In particular, $\phi^*(n) = 0$ if $(n, f_\Delta) \neq 1$, and

$$\mathbf{1}^*(n) = \mathsf{R}_\Delta(n) = \big|\{\mathfrak{a} \in \mathcal{J}_\Delta^* \mid \mathfrak{N}_\Delta(\mathfrak{a}) = n\}\big| \quad \text{for all} \quad n \in \mathbb{N}\,.$$

Lemma 8.2.1. *Let Δ be a quadratic discriminant and $\phi \in \mathfrak{C}_\Delta$ an ideal class character. Then $\phi(\mathfrak{a}\mathfrak{b}) = \phi(\mathfrak{a})\phi(\mathfrak{b})$ for all $\mathfrak{a}$, $\mathfrak{b} \in \mathcal{J}_\Delta^*$, and $\phi^* \colon \mathbb{N} \to \mathbb{C}$ is a multiplicative function.*

Proof. If $\mathfrak{a}$, $\mathfrak{b} \in \mathcal{J}_\Delta^*$, then

$$\phi(\mathfrak{a}\mathfrak{b}) = \phi([\mathfrak{a}\mathfrak{b}]^+) = \phi([\mathfrak{a}]^+[\mathfrak{b}]^+) = \phi([\mathfrak{a}]^+)\phi([\mathfrak{b}]^+) = \phi(\mathfrak{a})\phi(\mathfrak{b})\,.$$

If m_1, $m_2 \in \mathbb{N}$ and $(m_1, m_2) = 1$, then

$$\{\mathfrak{a} \in \mathcal{J}_\Delta^* \mid \mathfrak{N}_\Delta(\mathfrak{a}) = m_1 m_2\} = \{\mathfrak{a}_1\mathfrak{a}_2 \mid \mathfrak{a}_i \in \mathcal{J}_\Delta^*\,,\ \mathfrak{N}_\Delta(\mathfrak{a}_i) = m_i \text{ for } i \in \{1,2\}\}\,,$$

since every $\mathfrak{a} \in \mathcal{J}_\Delta^*$ has a unique factorization into prime ideal powers. Hence

$$\begin{aligned} \phi^*(m_1 m_2) &= \sum_{\substack{\mathfrak{a} \in \mathcal{J}_\Delta^* \\ \mathfrak{N}_\Delta(\mathfrak{a}) = m_1 m_2}} \phi(\mathfrak{a}) = \sum_{\substack{\mathfrak{a}_1 \in \mathcal{J}_\Delta^* \\ \mathfrak{N}_\Delta(\mathfrak{a}_1) = m_1}} \sum_{\substack{\mathfrak{a}_2 \in \mathcal{J}_\Delta^* \\ \mathfrak{N}_\Delta(\mathfrak{a}_2) = m_2}} \phi(\mathfrak{a}_1\mathfrak{a}_2) \\ &= \sum_{\substack{\mathfrak{a}_1 \in \mathcal{J}_\Delta^* \\ \mathfrak{N}_\Delta(\mathfrak{a}_1) = m_1}} \phi(\mathfrak{a}_1) \sum_{\substack{\mathfrak{a}_2 \in \mathcal{J}_\Delta^* \\ \mathfrak{N}_\Delta(\mathfrak{a}_2) = m_2}} \phi(\mathfrak{a}_2) = \phi^*(m_1)\phi^*(m_2)\,, \end{aligned}$$

and therefore ϕ^* is a multiplicative function. □

In the following Theorem 8.2.2 we introduce and investigate the Dirichlet series responsible for the analytic theory of quadratic orders.

Theorem 8.2.2. *Let* Δ *be a quadratic discriminant with conductor* f_Δ *and* $\phi \in \mathfrak{C}_\Delta$ *an ideal class character.*

1. *The Dirichlet series*

$$L_\Delta(s,\phi) = \sum_{\mathfrak{a}\in\mathcal{J}_\Delta^*} \frac{\phi(\mathfrak{a})}{\mathfrak{N}_\Delta(\mathfrak{a})^s} = \sum_{n=1}^\infty \frac{\phi^*(n)}{n^s} \quad \text{and} \quad \Lambda_\Delta(s,\phi) = \sum_{\mathfrak{p}\in\mathcal{P}_\Delta}\sum_{j=1}^\infty \frac{\phi(\mathfrak{p})^j}{j\mathfrak{N}_\Delta(\mathfrak{p})^{js}}$$

converge for all $s \in \mathcal{H}_1$ *and define holomorphic functions*

$$L_\Delta(\,\cdot\,,\phi)\colon \mathcal{H}_1 \to \mathbb{C} \quad \text{and} \quad \Lambda_\Delta(\,\cdot\,,\phi)\colon \mathcal{H}_1 \to \mathbb{C}\,.$$

2. *For* $s \in \mathcal{H}_1$*, we have*

$$L_\Delta(s,\phi) = \prod_{\mathfrak{p}\in\mathcal{P}_\Delta}\Bigl(1-\frac{\phi(\mathfrak{p})}{\mathfrak{N}_\Delta(\mathfrak{p})^s}\Bigr)^{-1} = \exp(\Lambda_\Delta(s,\phi))\,,$$

$$\zeta_\Delta(s) = L_\Delta(s,\mathbf{1}) = \sum_{\mathfrak{a}\in\mathcal{J}_\Delta^*}\frac{1}{\mathfrak{N}_\Delta(\mathfrak{a})^s} = \zeta(s)L(s,\mathsf{Q}_\Delta)\prod_{p\,|\,f_\Delta}\Bigl(1-\frac{1}{p^s}\Bigr)\,,$$

and if $s \in \mathbb{R}_{>1}$*, then*

$$\prod_{\psi\in\mathfrak{C}_\Delta} L_\Delta(s,\psi) \ge 1\,.$$

Proof. Let p be a prime, $\phi \in \mathfrak{C}_\Delta$, $s \in \mathcal{H}_1$ and $\sigma = \Re(s)$. We observe that $|p^s| = p^\sigma$, and we calculate the sums

$$\sum_{j=0}^\infty\Bigl|\frac{\phi^*(p^j)}{p^{js}}\Bigr| \quad \text{and} \quad \sum_{j=0}^\infty\frac{\phi^*(p^j)}{p^{js}}\,.$$

- If $p\,|\,f_\Delta$, then $\phi^*(p^j) = 0$ for all $j \in \mathbb{N}_0$.
- If $p\,|\,\Delta$ and $p \nmid f_\Delta$, then $p\mathcal{O}_\Delta = \mathfrak{p}^2$ for some $\mathfrak{p} \in \mathcal{P}_\Delta$, $\mathfrak{N}_\Delta(\mathfrak{p}) = p$, and $\phi^*(p^j) = \phi(\mathfrak{p}^j)$ for all $j \in \mathbb{N}_0$. Hence we obtain

$$\sum_{j=0}^\infty\Bigl|\frac{\phi^*(p^j)}{p^{js}}\Bigr| = \sum_{j=0}^\infty\frac{1}{p^{j\sigma}} = \Bigl(1-\frac{1}{p^\sigma}\Bigr)^{-1}$$

  and

$$\sum_{j=0}^\infty\frac{\phi^*(p^j)}{p^{js}} = \sum_{j=0}^\infty\frac{\phi(\mathfrak{p})^j}{\mathfrak{N}_\Delta(\mathfrak{p})^{js}} = \Bigl(1-\frac{\phi(\mathfrak{p})}{\mathfrak{N}_\Delta(\mathfrak{p})^s}\Bigr)^{-1}.$$

- If $\mathsf{Q}_\Delta(p) = -1$, then $\mathfrak{p} = p\mathcal{O}_\Delta \in \mathcal{P}_\Delta$, $\mathfrak{N}_\Delta(\mathfrak{p}) = p^2$, and if $j \in \mathbb{N}_0$, then

$$\phi^*(p^j) = \begin{cases} \phi(\mathfrak{p}^\nu) & \text{if } \ j = 2\nu\,, \\ 0 & \text{if } \ j \ \text{ is odd.}\end{cases}$$

Hence we obtain

$$\sum_{j=0}^{\infty}\Big|\frac{\phi^*(p^j)}{p^{js}}\Big| \;=\; \sum_{\nu=0}^{\infty}\frac{1}{p^{2\nu\sigma}} \;=\; \Big(1-\frac{1}{p^{2\sigma}}\Big)^{-1}$$

and

$$\sum_{j=0}^{\infty}\frac{\phi^*(p^j)}{p^{js}} \;=\; \sum_{\nu=0}^{\infty}\frac{\phi(\mathfrak{p}^\nu)}{\mathfrak{N}_\Delta(\mathfrak{p})^{\nu s}} = \sum_{\nu=0}^{\infty}\frac{\phi(\mathfrak{p})^\nu}{\mathfrak{N}_\Delta(\mathfrak{p})^{\nu s}} \;=\; \Big(1-\frac{\phi(\mathfrak{p})}{\mathfrak{N}_\Delta(\mathfrak{p})^{s}}\Big)^{-1}.$$

- If $\mathsf{Q}_\Delta(p)=1$, then $p\mathcal{O}_\Delta=\mathfrak{p}\mathfrak{p}'$, where $\mathfrak{p},\,\mathfrak{p}'\in\mathcal{P}_\Delta$, $\mathfrak{N}_\Delta(\mathfrak{p})=\mathfrak{N}_\Delta(\mathfrak{p}')=p$,

  $$\phi^*(p^j)=\sum_{\nu=0}^{j}\phi(\mathfrak{p}^\nu)\phi(\mathfrak{p}'^{j-\nu}),$$

  $\mathbf{1}^*(p^j)=j+1$ and $|\phi^*(p^j)|\le j+1$ for all $j\in\mathbb{N}_0$. Hence it follows that

  $$\sum_{j=0}^{\infty}\Big|\frac{\phi^*(p^j)}{p^{js}}\Big|\le\sum_{j=0}^{\infty}\frac{j+1}{p^{\nu\sigma}}=\Big(\sum_{j=0}^{\infty}\frac{1}{p^{j\sigma}}\Big)^2=\;\Big(1-\frac{1}{p^{\sigma}}\Big)^{-2}$$

  with equality if $\phi=\mathbf{1}$, and

  $$\sum_{j=0}^{\infty}\frac{\phi^*(p^j)}{p^{js}}=\sum_{j=0}^{\infty}\sum_{\nu=0}^{j}\frac{\phi(\mathfrak{p}^\nu)}{p^{\nu s}}\frac{\phi(\mathfrak{p}'^{j-\nu})}{p^{(j-\nu)s}}=\Big(\sum_{j=0}^{\infty}\frac{\phi(\mathfrak{p})^j}{\mathfrak{N}_\Delta(\mathfrak{p})^{js}}\Big)\Big(\sum_{j=0}^{\infty}\frac{\phi(\mathfrak{p}')^j}{\mathfrak{N}_\Delta(\mathfrak{p}')^{js}}\Big)$$
  $$=\Big(1-\frac{\phi(\mathfrak{p})}{\mathfrak{N}_\Delta(\mathfrak{p})^{s}}\Big)^{-1}\Big(1-\frac{\phi(\mathfrak{p}')}{\mathfrak{N}_\Delta(\mathfrak{p}')^{s}}\Big)^{-1}.$$

Consequently, we have proved that, for all $s\in\mathcal{H}_1$ with $\sigma=\Re(s)$,

$$\begin{aligned}\prod_{p\in\mathbb{P}}\Big(\sum_{j=0}^{\infty}\Big|\frac{\phi^*(p^j)}{p^{js}}\Big|\Big) &\le \prod_{\substack{p\in\mathbb{P}\\ p\,|\,\Delta,\,p\nmid f_\Delta}}\Big(1-\frac{1}{p^{\sigma}}\Big)^{-1}\prod_{\substack{p\in\mathbb{P}\\ \mathsf{Q}_\Delta(p)=-1}}\Big(1-\frac{1}{p^{2\sigma}}\Big)^{-1}\prod_{\substack{p\in\mathbb{P}\\ \mathsf{Q}_\Delta(p)=1}}\Big(1-\frac{1}{p^{\sigma}}\Big)^{-2}\\ &=\zeta(\sigma)\prod_{\substack{p\in\mathbb{P}\\ \mathsf{Q}_\Delta(p)=-1}}\Big(1+\frac{1}{p^{\sigma}}\Big)^{-1}\prod_{\substack{p\in\mathbb{P}\\ \mathsf{Q}_\Delta(p)=1}}\Big(1-\frac{1}{p^{\sigma}}\Big)^{-1}\prod_{\substack{p\in\mathbb{P}\\ p\,|\,f_\Delta}}\Big(1-\frac{1}{p^{\sigma}}\Big)\\ &=\zeta(\sigma)L(\sigma,\mathsf{Q}_\Delta)\prod_{\substack{p\in\mathbb{P}\\ p\,|\,f_\Delta}}\Big(1-\frac{1}{p^{\sigma}}\Big)\in\mathbb{R}_{>0}\,,\quad\text{with equality if }\phi=\mathbf{1}.\end{aligned}$$

Now we apply Theorem 4.2.4.1. First, for $s\in\mathcal{H}_1$ we have

$$\sum_{n=1}^{\infty}\Big|\frac{\phi^*(n)|}{n^s}\Big|=\prod_{p\in\mathbb{P}}\Big(\sum_{j=0}^{\infty}\Big|\frac{\phi^*(p^j)}{p^{js}}\Big|\Big)<\infty\,,$$

and therefore (by Lemma B.2.2) the Dirichlet series defining $L_\Delta(s,\chi)$ and $\Lambda_\Delta(s,\chi)$ converge for $s\in\mathcal{H}_1$ and define holomorphic functions $L_\Delta(\,\cdot\,,\phi)\colon\mathcal{H}_1\to\mathbb{C}$ and $\Lambda_\Delta(\,\cdot\,,\phi)\colon\mathcal{H}_1\to\mathbb{C}$. Next, it follows that, for all $s\in\mathcal{H}_1$,

$$\prod_{\mathfrak{p}\in\mathcal{P}_K}\Big(1-\frac{\phi(\mathfrak{p})}{\mathfrak{N}_\Delta(\mathfrak{p})^{s}}\Big)^{-1}=\prod_{p\in\mathbb{P}}\Big(\sum_{j=0}^{\infty}\frac{\phi^*(p^j)}{p^{js}}\Big)=\sum_{n=1}^{\infty}\frac{\phi^*\,(n)}{n^s}=L_\Delta(s,\phi)\,,$$

$$\zeta_\Delta(s) = L_\Delta(s,\mathbf{1}) = \prod_{p\in\mathbb{P}} \Bigg(\sum_{j=0}^\infty \frac{\mathsf{R}_\Delta(p^j)}{p^{js}}\Bigg) = \zeta(s)L(s,\mathsf{Q}_\Delta) \prod_{\substack{p\in\mathbb{P}\\ p\,|\,f_\Delta}} \Big(1-\frac{1}{p^s}\Big),$$

and

$$\exp(\Lambda_\Delta(s,\phi)) = \prod_{\mathfrak{p}\in\mathcal{P}_\Delta} \exp\Big(\sum_{j=1}^\infty \frac{\phi(\mathfrak{p})^j}{j\mathfrak{N}_\Delta(\mathfrak{p})^{js}}\Big) = \prod_{\mathfrak{p}\in\mathcal{P}_\Delta} \Big(1-\frac{\phi(\mathfrak{p})}{\mathfrak{N}_\Delta(\mathfrak{p})^s}\Big)^{-1} = L_\Delta(s,\phi)\,.$$

Finally, if $s\in\mathbb{R}_{>1}$, then

$$\prod_{\psi\in\mathfrak{C}_\Delta} L_\Delta(s,\psi) = \exp\left\{\sum_{\mathfrak{p}\in\mathcal{P}_\Delta}\sum_{j=1}^\infty \Bigg(\sum_{\psi\in\mathfrak{C}_\Delta}\psi(\mathfrak{p}^j)\Bigg)\frac{1}{j\mathfrak{N}_\Delta(\mathfrak{p})^{js}}\right\} \ge 1\,,$$

since, for every $\mathfrak{p}\in\mathcal{P}_\Delta$ and $j\in\mathbb{N}$ we have

$$\sum_{\psi\in\mathfrak{C}_\Delta}\psi(\mathfrak{p}^j) = \sum_{\psi\in\mathfrak{C}_\Delta}\psi\big([\mathfrak{p}^j]^+\big) \in \{0,\,|\mathcal{C}_\Delta^+|\} \quad \text{by Theorem A.7.7.} \qquad \square$$

Definition 8.2.3. Let Δ be a quadratic discriminant and $\phi\in\mathfrak{C}_\Delta$ an ideal class character. The function

$$L(\,\cdot\,,\phi)\colon \mathcal{H}_1\to\mathbb{C}\,,\quad \text{defined by}\quad L(s,\phi) = \sum_{\mathfrak{a}\in\mathcal{I}_\Delta^*}\frac{\phi(\mathfrak{a})}{\mathfrak{N}_\Delta(\mathfrak{a})^s} = \prod_{\mathfrak{p}\in\mathcal{P}_\Delta}\Big(1-\frac{\phi(\mathfrak{p})}{\mathfrak{N}_\Delta(\mathfrak{p})^s}\Big)^{-1}$$

is called the *Dedekind-Landau L-function* of the order $\mathcal{O}_\Delta$ associated with the ideal class character ϕ. The function

$$\zeta_\Delta = L_\Delta(\,\cdot\,,\mathbf{1})\colon \mathcal{H}_1\to\mathbb{C}\,,\quad \text{given by}\quad \zeta_\Delta(s) = \sum_{\mathfrak{a}\in\mathcal{I}_\Delta^*}\frac{1}{\mathfrak{N}_\Delta(\mathfrak{a})^s} = \prod_{\mathfrak{p}\in\mathcal{P}_\Delta}\Big(1-\frac{1}{\mathfrak{N}_\Delta(\mathfrak{p})^s}\Big)^{-1}$$

is called the *Dedekind zeta function* of the order $\mathcal{O}_\Delta$. If K is a quadratic number field, then $\zeta_K=\zeta_{\Delta_K}$ is called the *Dedekind zeta function* of K.

For a (narrow) ideal class $C\in\mathcal{C}_\Delta^+$, we define the *class zeta function*

$$\zeta_C\colon\mathcal{H}_1\to\mathbb{C}\quad\text{by}\quad \zeta_C(s) = \sum_{\substack{\mathfrak{a}\in\mathcal{I}_\Delta^*\\ [\mathfrak{a}]^+=C}}\frac{1}{\mathfrak{N}_\Delta(\mathfrak{a})^s}\,.$$

Since

$$\sum_{\mathfrak{a}\in\mathcal{I}_\Delta^*}\frac{1}{\mathfrak{N}_\Delta(\mathfrak{a})^\sigma} < \infty \quad\text{for all}\quad \sigma\in\mathbb{R}_{>1}\,,$$

it follows by Lemma B.2.2 that $\zeta_C\colon\mathcal{H}_1\to\mathbb{C}$ is a holomorphic function. By the very definition, we obtain

$$\zeta_\Delta(s) = \sum_{C\in\mathcal{C}_\Delta^+}\zeta_C(s) \quad\text{and}\quad L_\Delta(s,\phi) = \sum_{C\in\mathcal{C}_\Delta^+}\phi(C)\zeta_C(s)\,.$$

Theorem 8.2.4. *Let* Δ *be a quadratic discriminant and* $C \in \mathcal{C}_\Delta^+$ *a narrow ideal class. Then there exists a differentiable function* $G_C \colon \mathcal{H}_0 \to \mathbb{C}$ *such that*

$$\zeta_C(s) = \lambda_\Delta \frac{\varphi(f_\Delta)}{f_\Delta} \frac{s}{s-1} + sG_C(s) \quad \textit{for all } s \in \mathcal{H}_1\,,$$

where

$$\lambda_\Delta = \frac{2\pi}{\mathsf{w}_\Delta \sqrt{|\Delta|}} \quad \textit{if} \ \ \Delta < 0\,, \qquad \textit{and} \qquad \lambda_\Delta = \frac{\log \varepsilon_\Delta^+}{\sqrt{\Delta}} \quad \textit{if} \ \ \Delta > 0\,.$$

In particular:

- ζ_C *has an extension to a holomorphic function* $\zeta_\Delta \colon \mathcal{H}_0 \setminus \{1\} \to \mathbb{C}$ *satisfying*
$$\lim_{s\to 1}(s-1)\zeta_C(s) = \lambda_\Delta \frac{\varphi(f_\Delta}{f_\Delta}\,.$$
- *We have*
$$\lim_{s\to 1}(s-1)\zeta_\Delta(s) = h_\Delta^+ \lambda_\Delta \frac{\varphi(f_\Delta)}{f_\Delta}\,.$$
- *If* $\phi \in \mathfrak{C}_\Delta \setminus \{\mathbf{1}\}$, *then* $L_\Delta(\,\cdot\,,\phi)$ *has an extension to a holomorphic function* $L_\Delta(\,\cdot\,,\phi) \colon \mathcal{H}_0 \to \mathbb{C}$.

Proof. By definition,

$$\zeta_C(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \big|\{\mathfrak{a} \in \mathcal{I}_\Delta^* \mid [\mathfrak{a}]^+ = C\,,\ \mathfrak{N}_\Delta(\mathfrak{a}) = n\}\big|\,,$$

and for $N \in \mathbb{N}$ we set

$$\mathsf{R}_C^*(N) = \sum_{n=1}^{N} \big|\{\mathfrak{a} \in \mathcal{I}_\Delta^* \,\big|\, [\mathfrak{a}]^+ = C,\ \mathfrak{N}_\Delta(\mathfrak{a}) = n\}\big| = \big|\{\mathfrak{a} \in \mathcal{I}_\Delta^* \,\big|\, [\mathfrak{a}]^+ = C,\ \mathfrak{N}_\Delta(\mathfrak{a}) \le N\}\big|\,.$$

By Theorem 8.1.3, there exists some $B \in \mathbb{R}_{>0}$ such that

$$\Big|\mathsf{R}_C^*(N) - \lambda_\Delta \frac{\varphi(f_\Delta)}{f_\Delta} N\Big| \le B\sqrt{N} \quad \text{for all} \quad N \in \mathbb{N}\,,$$

and Theorem B.2.5 implies the existence of a holomorphic function G_C with the desired properties. In particular, ζ_C has an extension to a holomorphic function $\zeta_\Delta \colon \mathcal{H}_0 \setminus \{1\} \to \mathbb{C}$ satisfying

$$\lim_{s\to 1}(s-1)\zeta_C(s) = \lambda_\Delta \frac{\varphi(f_\Delta)}{f_\Delta}\,,$$

and

$$\lim_{s\to 1}(s-1)\zeta_\Delta(s) = \sum_{C\in\mathcal{C}_\Delta^+} \lim_{s\to 1}(s-1)\zeta_C(s) = h_\Delta^+ \lambda_\Delta \frac{\varphi(f_\Delta)}{f_\Delta}\,.$$

If $\phi \in \mathfrak{C}_\Delta \setminus \{\mathbf{1}\}$, then (by Theorem A.7.7)

$$\begin{aligned} L_\Delta(s,\phi) = \sum_{C \in \mathcal{C}_\Delta^+} \phi(C)\zeta_C(s) = {}& \lambda_\Delta \frac{\varphi(f_\Delta)}{f_\Delta}\,\frac{s}{s-1} \sum_{C \in \mathcal{C}_\Delta^+} \phi(C) + \sum_{C \in \mathcal{C}_\Delta^+} \phi(C) s G_C(s) \\ = {}& \sum_{C \in \mathcal{C}_\Delta^+} \phi(C) s G_C(s) \quad \text{for all} \quad s \in \mathcal{H}_1\,. \end{aligned}$$

□

Theorem 8.2.5. *If Δ be a quadratic discriminant and $\phi \in \mathfrak{C}_\Delta \setminus \{\mathbf{1}\}$ is an ideal class character, the $L_\Delta(1,\phi) \ne 0$.*

Proof. Assume to the contrary that $L(1,\psi) = 0$ for some ideal class character $\psi \in \mathfrak{C}_\Delta \setminus \{\mathbf{1}\}$.

CASE 1: $\psi \ne \overline{\psi}$. Suppose that $s \in \mathbb{R}_{>1}$, and observe that $\overline{\psi} \in \mathfrak{C}_\Delta \setminus \{\mathbf{1}\}$. Since $L_\Delta(s,\overline{\psi}) = \overline{L_\Delta(s,\psi)}$ and $L_\Delta(\,\cdot\,,\psi)$ is differentiable in 1, there exists a continuous function $G\colon \mathbb{R}_{>0} \to \mathbb{C}$ such that $L_\Delta(s,\psi) = (s-1)G(s)$ and $L(s,\overline{\psi}) = (s-1)\overline{G(s)}$. By Theorem 8.2.2.2, it follows that

$$1 \le \prod_{\phi \in \mathfrak{C}_\Delta} L_\Delta(s,\phi) = \zeta_\Delta(s) L_\Delta(s,\phi) L_\Delta(s,\overline{\psi}) F(s) = \zeta_\Delta(s)(s-1)^2 |G(s)|^2 F(s)\,,$$

where

$$F(s) = \prod_{\phi \in \mathfrak{C}_\Delta \setminus \{\mathbf{1},\psi,\overline{\psi}\}} L_\Delta(s,\psi)\,.$$

Since $F\colon \mathbb{R}_{>0} \to \mathbb{C}$ is a differentiable function, we obtain

$$\lim_{s \to 1+} (s-1)|G(s)|^2 F(s) = 0\,, \quad \text{and as} \quad \lim_{s \to 1+} (s-1)\zeta_\Delta(s) \in \mathbb{R}_{>0}\,,$$

we arrive at a contradiction.

CASE 2: $\psi = \overline{\psi}$. The function $\Psi\colon \mathbb{R}_{1/2} \to \mathbb{C}$, defined by

$$\Psi(s) = \frac{\zeta_\Delta(s) L_\Delta(s,\phi)}{\zeta_\Delta(2s)}\,, \quad \text{is holomorphic,} \quad \lim_{s \to 1/2+} \Psi(s) = \infty\,,$$

and by Theorem 4.2.4 we obtain for all $s \in \mathcal{H}_1$

$$\begin{aligned} \Psi(s) &= \prod_{\mathfrak{p} \in \mathcal{P}_\Delta} \frac{1 - \mathfrak{N}_\Delta(\mathfrak{p})^{-2s}}{(1 - \mathfrak{N}_\Delta(\mathfrak{p})^{-s})(1 - \phi(\mathfrak{p})\mathfrak{N}_\Delta(\mathfrak{p})^{-s})} = \prod_{\mathfrak{p} \in \mathcal{P}_\Delta} \frac{1 + \mathfrak{N}_\Delta(\mathfrak{p})^{-s}}{1 - \phi(\mathfrak{p})\mathfrak{N}_\Delta(\mathfrak{p})^{-s}} \\ &= \prod_{\substack{\mathfrak{p} \in \mathcal{P}_\Delta \\ \phi(\mathfrak{p}) = 1}} \frac{1 + \mathfrak{N}_\Delta(\mathfrak{p})^{-s}}{1 - \mathfrak{N}_\Delta(\mathfrak{p})^{-s}} = \prod_{\substack{\mathfrak{p} \in \mathcal{P}_\Delta \\ \phi(\mathfrak{p}) = 1}} \left(1 + 2\sum_{n=1}^{\infty} \frac{1}{\mathfrak{N}_\Delta(\mathfrak{p})^{ns}}\right) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}\,, \end{aligned}$$

where $f\colon \mathbb{N} \to \mathbb{R}$ is the multiplicative function defined for prime powers $p^k > 1$ by

$$f(p^k) = 2\,|\{\mathfrak{p} \in \mathcal{P}_\Delta \mid \mathfrak{N}_\Delta(\mathfrak{p}^n) = p^k \ \text{ for some } \ n \in \mathbb{N}\}|\,.$$

The Taylor expansion of Ψ with center $s = 2$ shows that

$$\Psi(s) = \sum_{k=0}^{\infty} \frac{\Psi^{(k)}(2)}{k!}\,(s-2)^k = \sum_{k=0}^{\infty} \frac{1}{k!} \sum_{n=1}^{\infty} \frac{f(n)(\log n)^k}{n^2} (2-s)^k \quad \text{for all} \quad s \in (1/2, 2]\,,$$

and that $\Psi\colon (1/2, 2] \to \mathbb{R}$ is monotonically decreasing, a contradiction. □

We apply our investigations of the Dedekind-Landau L-functions to prove a quadratic analog to Dirichlet's prime number theorem. Our procedure is similar to that in Section 4.4.

Theorem 8.2.6. *Let Δ be a quadratic discriminant and $\phi \in \mathfrak{C}_\Delta$ an ideal class character. For real $s \in \mathbb{R}_{>1}$ tending to 1, the functions $\Lambda_\Delta(s,\phi)$ behaves as follows:*

$$\lim_{s\to 1+} \Lambda_\Delta(s,\phi) \ \text{ exists in } \mathbb{C} \ \text{ if } \ \phi \ne \mathbf{1}, \ \text{ and } \ \lim_{s\to 1+} \Lambda_\Delta(s,\mathbf{1}) = \infty\,.$$

Proof. Theorem 8.2.4 implies

$$\lim_{s\to 1+}(s-1)\zeta_\Delta(s) = h_\Delta^+\lambda_\Delta\frac{\varphi(f_\Delta)}{f_\Delta}\,, \quad \text{hence} \quad \lim_{s\to 1+}\zeta_\Delta(s) = \infty\,.$$

Since $\Lambda_\Delta(s,\mathbf{1}) \in \mathbb{R}$ and $L_\Delta(s,\mathbf{1}) = \exp\Lambda_\Delta(s,\mathbf{1})$ for all $s \in \mathbb{R}_{>1}$, it follows that also

$$\lim_{s\to 1+}\Lambda_\Delta(s,\mathbf{1}) = \infty\,.$$

Assume now that $\phi \ne \mathbf{1}$. Then $L_\Delta(1,\phi) \ne 0$ by Theorem 8.2.5, hence there exists some $b \in \mathbb{C}$ such that $L_\Delta(1,\phi) = \mathsf{e}^b$, and we define

$$h\colon \mathbb{R}_{>1} \to \mathbb{C} \quad \text{by} \quad h(s) = 1 - \mathsf{e}^{-b}L_\Delta(s,\phi)\,.$$

Since $L_\Delta(\,\cdot\,,\phi)\colon \mathbb{R}_{>0} \to \mathbb{C}$ is continuous, there exist ε, $\theta \in (0,1)$ such that $|h(s)| \le \theta$ for all $s \in (1-\varepsilon, 1+\varepsilon)$, h is continuous, and we define $H\colon (1-\varepsilon,1+\varepsilon) \to \mathbb{C}$ by

$$H(s) = \sum_{j=1}^\infty \frac{h(s)^j}{j}\,.$$

This series is uniformly convergent, hence Φ is continuous, and if $s \in (1, 1+\varepsilon)$, then

$$\mathsf{e}^{H(s)} = \frac{1}{1-h(s)} = \frac{\mathsf{e}^b}{L_\Delta(s,\phi)} = \mathsf{e}^{b-\Lambda_\Delta(s,\phi)}\,.$$

The function $K\colon (1,1+\varepsilon) \to \mathbb{C}$, defined by $K = H(s) - b + \Lambda_\Delta(s,\phi)$, is continuous, and as $\mathsf{e}^{K(s)} = 1$, it follows that $L(s) \in 2\pi\mathsf{i}\mathbb{Z}$ or all $s \in (1, 1+\varepsilon)$. Hence K is constant, say $K(s) = c \in \mathbb{C}$ for all $s \in (1,1+\varepsilon)$, and

$$\lim_{s\to 1+}\Lambda_\Delta(s,\phi) = \lim_{s\to 1+}[\,K(s) - H(s) + b\,] = c - H(1) + b \in \mathbb{C}\,. \qquad \square$$

Theorem 8.2.7. *Let Δ be a quadratic discriminant. Then every (narrow) ideal class $C \in \mathcal{C}_\Delta^+$ contains infinitely many prime ideals $\mathfrak{p}$ such that $\mathfrak{N}_\Delta(\mathfrak{p})$ is a prime.*

Proof. Now let $\mathcal{P}_\Delta^1$ be the set of all $\mathfrak{p} \in \mathcal{P}_\Delta$ such that $\mathfrak{N}_\Delta(\mathfrak{p})$ is a prime, and let $C \in \mathcal{C}_\Delta^+$ be a narrow ideal class. We must prove that the set $\mathcal{P}_\Delta^1 \cap C$ (consisting of all non-zero prime ideals $\mathfrak{p} \in \mathcal{P}_\Delta^1$ such that $(\mathfrak{N}_\Delta(\mathfrak{p}), f_\Delta) = 1$ and $[\mathfrak{p}]^+ = C$) is infinite. For $s \in \mathbb{R}_{>1}$, we set

$$\pi_C(s) = \sum_{\mathfrak{p}\in\mathcal{P}_\Delta\cap C}\frac{1}{\mathfrak{N}_\Delta(\mathfrak{p})^s}\,, \qquad \Pi_C(s) = \sum_{\phi\in\mathfrak{C}_\Delta}\overline{\phi}(C)\Lambda_\Delta(s,\phi)\,,$$

and we obtain

$$\begin{aligned}\Pi_C(s) &= \sum_{\mathfrak{p}\in\mathcal{P}_\Delta}\sum_{\phi\in\mathfrak{C}_\Delta}\overline{\phi}(C)\frac{\phi(\mathfrak{p})}{\mathfrak{N}_\Delta(\mathfrak{p})^s} + \sum_{\mathfrak{p}\in\mathcal{P}_\Delta}\sum_{j=2}^{\infty}\sum_{\phi\in\mathfrak{C}_\Delta}\overline{\phi}(C)\frac{\phi(\mathfrak{p})^j}{\mathfrak{N}_\Delta(\mathfrak{p})^{js}}\\ &= h_\Delta^+\pi_C(s) + \sum_{\phi\in\mathfrak{C}_\Delta}G_\phi(s)\,, \quad \text{where} \quad G_\phi(s) = \sum_{\mathfrak{p}\in\mathcal{P}_\Delta}\sum_{j=2}^{\infty}\overline{\phi}(C)\frac{\phi(\mathfrak{p}^j)}{\mathfrak{N}_\Delta(\mathfrak{p})^{sj}}\,.\end{aligned}$$

If $\phi\in\mathfrak{C}_\Delta$ and $s\ge\vartheta>\frac{1}{2}$, then

$$\begin{aligned}|G_\phi(s)| &\le \sum_{\mathfrak{p}\in\mathcal{P}_\Delta}\sum_{j=2}^{\infty}\frac{1}{\mathfrak{N}_\Delta(\mathfrak{p})^{\vartheta j}} = \sum_{\mathfrak{p}\in\mathcal{P}_\Delta}\frac{1}{\mathfrak{N}_\Delta(\mathfrak{p})^{2\vartheta}}\,\frac{1}{1-\mathfrak{N}_\Delta(\mathfrak{p})^{-\vartheta}}\\ &\le \frac{1}{1-2^{-\vartheta}}\sum_{\mathfrak{p}\in\mathcal{P}_\Delta}\frac{1}{\mathfrak{N}_\Delta(\mathfrak{p})^{2\vartheta}} \;<\infty\,.\end{aligned}$$

Hence the series defining the functions G_ϕ are absolutely and uniformly convergent in $\mathbb{R}_{\ge\vartheta}$, and therefore the functions G_ϕ are continuous in 1. For $s\in\mathbb{R}_{>1}$, we obtain

$$\pi_C(s) = \frac{1}{h_\Delta^+}\left[\Lambda_\Delta(s,\mathbf{1})+H(s)\right], \quad \text{where} \;\; H(s) = \sum_{\phi\in\mathfrak{C}_\Delta\setminus\{\mathbf{1}\}}\overline{\phi}(C)\Lambda_\Delta(s,\phi)+\sum_{\phi\in\mathfrak{C}_\Delta}G_\phi(s)\,.$$

By Theorem 8.2.6,

$$\lim_{s\to1+}H(s) \;\text{ exists in } \mathbb{C} \quad \text{and} \quad \lim_{s\to1+}\Lambda(s,\mathbf{1})=\infty\,, \quad \text{hence} \quad \lim_{s\to1+}\pi_C(s)=\infty\,.$$

If $\mathfrak{p}\in\mathcal{P}_\Delta\setminus\mathcal{P}_\Delta^1$, then $\mathfrak{N}_\Delta(\mathfrak{p})=p^2$ for some prime p, and therefore

$$\sum_{\mathfrak{p}\in\mathcal{P}_\Delta\setminus\mathcal{P}_\Delta^1}\frac{1}{\mathfrak{N}_\Delta(\mathfrak{p})} \;\le\; \sum_{p\in\mathbb{P}}\frac{1}{p^2}<\infty\,.$$

Since

$$\pi_C(s) = \sum_{\mathfrak{p}\in\mathcal{P}_\Delta^1\cap C}\frac{1}{\mathfrak{N}_\Delta(\mathfrak{p})^s} + \sum_{\mathfrak{p}\in(\mathcal{P}_\Delta\setminus\mathcal{P}_\Delta^1)\cap C}\frac{1}{\mathfrak{N}_\Delta(\mathfrak{p})^s} \qquad \text{and} \quad \sum_{\mathfrak{p}\in(\mathcal{P}_\Delta\setminus\mathcal{P}_\Delta^1)\cap C}\frac{1}{\mathfrak{N}_\Delta(\mathfrak{p})}<\infty\,,$$

it follows that

$$\lim_{s\to1+}\sum_{\mathfrak{p}\in\mathcal{P}_\Delta^1\cap C}\frac{1}{\mathfrak{N}_\Delta(\mathfrak{p})^s}=\infty\,,$$

which implies that the set $\mathcal{P}_\Delta^1\cap C$ is infinite. □

We close this section with an application to binary quadratic forms which we already announced several times.

Theorem 8.2.8. *Let Δ be a quadratic discriminant and f a not negative definite primitive form. Then f represents infinitely many primes.*

PROOF. Let $F=[\![f]\!]\in\mathfrak{F}_\Delta$ be the class of f and consider the bijective map $\Phi_\Delta\colon\mathfrak{F}_\Delta\to\mathcal{C}_\Delta^+$ given by Theorem 6.4.2. By Theorem 6.4.13.1, F (and thus f) represents a prime p if and only if $p=\mathfrak{N}_\Delta(\mathfrak{p})$ for some prime ideal $\mathfrak{p}\in\Phi_\Delta(F)$. But by Theorem 8.2.7, the set of prime ideal $\mathfrak{p}\in\Phi_\Delta(F)$ such that $\mathfrak{N}_\Delta(\mathfrak{p})$ is a prime is infinite. □

8.3. Ambiguous classes and classes of order divisibility by 4

Let Δ be a quadratic discriminant. We consider the isomorphism

$$\Phi_\Delta \colon \mathfrak{F}_\Delta \overset{\sim}{\to} \mathcal{C}^+_\Delta ,$$

given by Theorem and Definition 6.4.2 as follows: If $f = [a, b, c]$ is a not negative definite primitive form of discriminant Δ, then

$$\Phi_\Delta(\llbracket f \rrbracket) = \begin{cases} [\mathfrak{a}_f]^+ & \text{if} \quad a > 0 , \\ [\mathfrak{a}_f\sqrt{\Delta}\,]^+ & \text{if} \quad a < 0 , \end{cases} \qquad \text{where} \quad \mathfrak{a}_f = \Big[a, \frac{b+\sqrt{\Delta}}{2} \Big] \subset \mathcal{O}_\Delta .$$

Φ_Δ induces an isomorphism $(\Phi_\Delta)_2 \colon (\mathfrak{F}_\Delta)_2 \to (\mathcal{C}^+_\Delta)_2$ of the 2-components, which we call the 2-*class groups*. In this and the following sections we investigate discriminants with a cyclic 2-class group and we shall give explicit criteria for the divisibility by 4, 8 and 16. We call by $\mathfrak{A}_\Delta = \mathfrak{F}_\Delta[2] = \{F \in \mathfrak{F}_\Delta \mid F^2 = H_\Delta\}$ the *ambiguous form class group* (recall that we denote by $H_\Delta \in \mathfrak{F}_\Delta$ the principal class). A form f and also its class $\llbracket f \rrbracket$ are called *ambiguous* if $\llbracket f \rrbracket \in \mathfrak{A}_\Delta$. Φ_Δ induces isomorphisms

$$\mathfrak{F}_\Delta/\mathfrak{F}_\Delta^2 \overset{\sim}{\to} \mathcal{C}^+_\Delta/\mathcal{C}^{+2}_\Delta \quad \text{and} \quad \mathfrak{A}_\Delta \overset{\sim}{\to} \mathcal{A}^+_\Delta = \mathcal{C}^+_\Delta[2] .$$

By Theorem 5.6.11 we obtain $|\mathfrak{A}_\Delta| = |\mathcal{A}^+_\Delta| = 2^{\mu(\Delta)-1}$, and $\mathsf{r}_2(\mathfrak{F}_\Delta) = \mu_\Delta - 1$ is the 2-rank of $\mathfrak{F}_\Delta$.

Next we observe that for the study of the 2-class group it suffices to consider even discriminants. Indeed, let $\Delta \equiv 1 \bmod 4$ be an odd discriminant. By Theorem 6.4.14 there is an epimorphism $\Theta \colon \mathfrak{F}_{4\Delta} \to \mathfrak{F}_\Delta$ such that $|\mathrm{Ker}(\Theta)| \in \{1, 3\}$, and, by Theorem A.5.6, Θ induces an isomorphism $\Theta_2 \colon (\mathfrak{F}_{4\Delta})_2 \overset{\sim}{\to} (\mathfrak{F}_\Delta)_2$ of the 2-class groups.

Already in Theorem 5.6.13 we gave criteria for $(\mathcal{C}^+_\Delta)_2$ (and thus for $(\mathfrak{F}_\Delta)_2$) to be trivial. The previous observations allow us to characterize discriminants with a non-trivial cyclic 2-class group.

Theorem 8.3.1. *Let* $\Delta = 4D$ *be an even quadratic discriminant. Then the following assertions are equivalent*:

(a) *The* 2*-class group* $(\mathfrak{F}_\Delta)_2$ *is non-trivial and cyclic.*

(b) $|\mathfrak{A}_\Delta| = 2$.

(c) $\mu(\Delta) = 2$.

(d) *One of the following assertions hold*:

- $D \equiv 1 \bmod 4$ *and* $D = \pm p^r q^s$ *for odd primes* $p \neq q$ *and* $r, s \in \mathbb{N}$.
- $D \equiv 3 \bmod 4$ *and* $D = \pm p^r$ *for an odd prime* p *and* $r \in \mathbb{N}$.
- $D \equiv 2 \bmod 4$ *and* $D = \pm 2p^r$ *for an odd prime* p *and* $r \in \mathbb{N}$.
- $D \equiv 4 \bmod 8$ *and* $D = \pm 4p^r$ *for an odd prime* p *and* $r \in \mathbb{N}$.
- $D = \pm 2^r$ *for some* $r \geq 3$.

PROOF. Obvious by the previous remarks and the definition of $\mu(\Delta)$. □

We want to describe ambiguous classes by means of ambiguous forms, and for this purpose we must introduce distinguished ambiguous forms.

Definition 8.3.2. Let $\Delta = 4D$ be an even quadratic discriminant.

A form f of discriminant Δ is called *simple ambiguous* if it is not negative definite and of one of the following two types.

Type (A): $f = [a, 0, c]$, where $a,\, c \in \mathbb{Z}$, $(a, c) = 1$, $D = -ac$ and $|a| \le |c|$.

Type (B): $f = [2a, 2|a|, c]$, where $a,\, c \in \mathbb{Z}$, $(2a, c) = 1$, $D = a(a - 2c)$ and $|a| \le |a - 2c|$.

Let f be a simple ambiguous form of discriminant Δ.

- If $f = [a, 0, c]$ is of type (A), then $\mathfrak{a}_f = [a, \sqrt{D}\,]$ is an ambiguous ideal of type (I) according to Theorem 5.6.4, and we set
$$\mathfrak{a}_f^* = [c, \sqrt{D}] = a^{-1}\sqrt{D}\,\mathfrak{a}_f\,.$$
If $\Delta > 0$, then $f^- = [-a, 0, -c]$ is also a simple ambiguous form of discriminant Δ, and $\mathfrak{a}_f = \mathfrak{a}_{f^-}$.
- If $f = [2a, 2|a|, c]$ is of type (B), then $\mathfrak{a}_f = [2a, a + \sqrt{D}\,]$ is an ambiguous ideal of type (II) according to Theorem 5.6.4, and we set
$$\mathfrak{a}_f^* = [2(a - 2c), a - 2c + \sqrt{D}\,] = a^{-1}\sqrt{D}\,\mathfrak{a}_f\,.$$
If $\Delta > 0$, then $f^- = [-2a, 2|a|, -c]$ is also a simple ambiguous form of discriminant Δ, and $\mathfrak{a}_f = \mathfrak{a}_{f^-}$.

In each case, we call a form $f = [a, 2b, c]$ *quasipositive* if $a > 0$.

Our next aim is to connect simple ambiguous forms with ambiguous pairs of ideals as introduced in Theorem 5.6.7.

Theorem 8.3.3. *Let $\Delta = 4D$ be an even quadratic discriminant, $\Delta \ne -4$.*

1. *If f is a simple ambiguous form of discriminant Δ, then $[\![f]\!] \in \mathfrak{A}_\Delta$ is an ambiguous class, and $(\mathfrak{a}_f, \mathfrak{a}_f^*)$ is an ambiguous pair in $\mathcal{O}_\Delta$. Conversely, if $(\mathfrak{a}, \mathfrak{a}^*)$ is an ambiguous pair in $\mathcal{O}_\Delta$, then there exists a simple ambiguous form f such that $(\mathfrak{a}, \mathfrak{a}^*) = (\mathfrak{a}_f, \mathfrak{a}_f^*)$. In fact, there is exactly one such form if $\Delta < 0$, and there are exactly two such forms if $\Delta > 0$, namely f and f^-.*
2. *Let $F \in \mathfrak{A}_\Delta$ be an ambiguous class of forms. If $\Delta < 0$, then F contains exactly one simple ambiguous form. If $\Delta > 0$, then F contains exactly two simple ambiguous forms f and f', where $f' = f^-$ if $\mathcal{N}(\varepsilon_\Delta) = -1$, and $f' \ne f^-$ if $\mathcal{N}(\varepsilon_\Delta) = 1$.*

PROOF. 1. If f is a simple ambiguous form of discriminant Δ, then $(\mathfrak{a}_f, \mathfrak{a}_f^*)$ is an ambiguous pair in $\mathcal{O}_\Delta$ by definition, and $\Phi_\Delta([\![f]\!]) \in \{[\mathfrak{a}_f]^+, [\mathfrak{a}_f\sqrt{\Delta}]^+\}$. Hence $\Phi_\Delta([\![f]\!])$ and thus also $[\![f]\!]$ itself is an ambiguous class.

Assume now that $(\mathfrak{a}, \mathfrak{a}^*)$ is an ambiguous pair in $\mathcal{O}_\Delta$, and apply Theorem 5.6.7.

CASE 1: $\mathfrak{a}$ is of type (I). Then $D = \varepsilon d d^*$, where $\varepsilon = \operatorname{sgn}(\Delta)$, $d,\, d^* \in \mathbb{N}$, $d < d^*$, $(d, d^*) = 1$, $\mathfrak{a} = [d, \sqrt{D}\,]$ and $\mathfrak{a}^* = [d^*, \sqrt{D}\,]$. Then $f = [d, 0, -\varepsilon d^*]$ is a simple ambiguous form of discriminant $\Delta = 4D$, and $(\mathfrak{a}, \mathfrak{a}^*) = (\mathfrak{a}_f, \mathfrak{a}_f^*)$. If f' is any simple ambiguous form of discriminant Δ such that $(\mathfrak{a},\mathfrak{a}^*)=(\mathfrak{a}_{f'},\mathfrak{a}^*_{f'})$, then f' is of type (A), say $f'=[a,0,c]$. Since $|a|\le|c|$, it follows that $|a|=|d|$ and $|c|=|d^*|$. If $\Delta<0$, then $a>0,\ c>0$, and therefore $f'=f$. If $\Delta>0$, then it follows that either $f'=f$ or $f'=[-d,0,\varepsilon d^*]=f^-$.

CASE 2 : $\mathfrak{a}$ is of type (II). Then $\Delta=\varepsilon dd^*$, where $\varepsilon=\operatorname{sgn}(\Delta)$, $d,\,d^*\in\mathbb{N}$, $d<d^*$, $d-\varepsilon d^*=4c$ for some $c\in\mathbb{Z}$ such that $(c,d)=1$,

$$\mathfrak{a}=\Bigl[d,\frac{d+\sqrt{\Delta}}{2}\Bigr]\quad\text{and}\quad\mathfrak{a}^*=\Bigl[d^*,\frac{d^*+\sqrt{\Delta}}{2}\Bigr].$$

Since $\Delta\equiv 0\bmod 4$ and $d\equiv d^*\bmod 2$, we obtain $d=2a$ for some $a\in\mathbb{N}$, hence $d^*=2\varepsilon(a-2c)$, $\mathfrak{a}=[2a,a+\sqrt{D}\,]$ and $\mathfrak{a}^*=[2(a-2c),a-2c+\sqrt{D}\,]$. The form $f=[2a,2|a|,c]$ is a simple ambiguous form of discriminant $\Delta=4D$, and $(\mathfrak{a},\mathfrak{a}^*)=(\mathfrak{a}_f,\mathfrak{a}^*_f)$. If f' is any simple ambiguous form of discriminant Δ such that $(\mathfrak{a},\mathfrak{a}^*)=(\mathfrak{a}_{f'},\mathfrak{a}^*_{f'})$, then f' is of type (B), say $f'=[2a',2|a'|,c']$. Since $|a'|\le|a'-2c'|$, it follows that $|a'|=|a|$ and $|c'|=|c|$. If $\Delta<0$, then $a>0,\ c>0$, and therefore $f'=f$. If $\Delta<0$, then it follows that either $f'=f$ or $f'=[-2a,2|a|,-c]=f^-$.

2. We consider the narrow ambiguous ideal class $C=\Phi_\Delta(F)$. A simple ambiguous form f belongs to F if and only if either f is quasipositive and $C=[\mathfrak{a}_f]^+$, or f is not quasipositive and $C=[\mathfrak{a}_f\sqrt{\Delta}\,]^+$. In the sequel. we apply Theorem 5.6.11.

CASE 1 : $\Delta<0$, or $\Delta>0$ and $\mathcal{N}(\varepsilon_\Delta)=-1$. In this case, $[\mathfrak{a}]^+=[\mathfrak{a}\sqrt{\Delta}\,]^+$ for every $\mathcal{O}_\Delta$-regular ambiguous ideal $\mathfrak{a}$, and C contains exactly one ambiguous pair $(\mathfrak{a},\mathfrak{a}^*)$. If f is a quasipositive simple ambiguous form such that $\mathfrak{a}=\mathfrak{a}_f$, then $C=[\mathfrak{a}_f]^+$, and thus $f\in F$. Let $f'\in F$ be any simple ambiguous form. Since $[\mathfrak{a}_{f'}]^+=[\mathfrak{a}_{f'}\sqrt{\Delta}\,]^+$, it follows that $(\mathfrak{a}_{f'},\mathfrak{a}^*_{f'})$ is an ambiguous pair in C, and therefore $\mathfrak{a}_{f'}=\mathfrak{a}_f$. By 1. we obtain $f'=f$ if $\Delta<0$, and $f'\in\{f,f^-\}$ if $\Delta>0$.

CASE 2 : $\Delta>0$ and $\mathcal{N}(\varepsilon_\Delta)=1$. In this case we have $C\ne\overline{C}=C[\sqrt{\Delta}\mathcal{O}_\Delta]^+$, $C\uplus\overline{C}\in\mathcal{A}_\Delta$, and $C\uplus\overline{C}$ contains exactly two ambiguous pairs, say $(\mathfrak{a}_1,\mathfrak{a}_1^*)$ and $(\mathfrak{a}_2,\mathfrak{a}_2^*)$. After renumbering (if necessary) we are in one of the following three cases :

a. $\{\mathfrak{a}_1,\mathfrak{a}_2\}\subset C$; **b.** $\{\mathfrak{a}_1^*,\mathfrak{a}_2^*\}\subset C$; **c.** $\{\mathfrak{a}_1,\mathfrak{a}_2^*\}\subset C$.

If f is any simple ambiguous form, then $\llbracket f\rrbracket\ne\llbracket f^-\rrbracket$ by Corollary 6.1.5. For $i\in\{1,2\}$, let f_i be a quasipositive simple ambiguous form such that $\mathfrak{a}_i=\mathfrak{a}_{f_i}$. If $\mathfrak{a}_i\in C$, then $f_i\in F$. If $\mathfrak{a}_i^*\in C$, then $\Phi_\Delta(\llbracket f_i^-\rrbracket)=[\mathfrak{a}_{f_i}\sqrt{\Delta}\,]^+=[\mathfrak{a}^*_{f_i}]^+=[\mathfrak{a}_i^*]^+=C$, and $f_i^-\in F$. Hence we obtain $\{f_1,f_2\}\subset F$ in case **a**, $\{f_1^-,f_2^-\}\subset F$ in case **b**, and $\{f_1,f_2^-\}\subset F$ in case **c.** If $f'\in F$ is any simple ambiguous form, then $(\mathfrak{a}_{f'},\mathfrak{a}^*_{f'})$ is an ambiguous pair in $C\uplus\overline{C}$, hence $(\mathfrak{a}_{f'},\mathfrak{a}^*_{f'})=(\mathfrak{a}_i,\mathfrak{a}_i^*)$ for some $i\in\{1,2\}$, which implies $f'\in\{f_i,f_i^-\}$. Hence in each case there are no other simple ambiguous forms in F. □

Corollary 8.3.4. *Let* $\Delta=4D$ *be an even quadratic discriminant such that the* 2*-class group* $(\mathfrak{F}_\Delta)_2$ *is non-trivial and cyclic* (see Theorem 8.3.1). *Suppose that* $g=[1,0,-D]$ *is the principal form,* $H=\llbracket g\rrbracket\in\mathfrak{F}_\Delta$ *is the principal class and* $A\in\mathfrak{F}_\Delta$ *is the unique non-principal ambiguous class.*

1. *If* $\Delta > 0$*, then there exist exactly three non-principal simple ambiguous forms of discriminant* Δ*, one lies in* H*, and the two others lie in* A*.*
2. *If* $\Delta < 0$*, then there exists exactly one non-principal simple ambiguous form* f *of discriminant* Δ*, and* $[\![f]\!] = A$*.*

PROOF. By Theorem 8.3.3.2. □

Now we make Corollary 8.3.4 explicit. We consider even quadratic discriminants $\Delta = 4D$ with a non-trivial cyclic 2-class group. From now on however, we restrict to the cases where D is squarefree. In these cases either $D \equiv 1 \bmod 4$ is a fundamental discriminant (and then $|(\mathcal{C}_\Delta^+)_2| = |(\mathcal{C}_D^+)_2|$), or $D \equiv 2$ or $3 \bmod 4$ and Δ is a fundamental discriminant. By Theorem 8.3.1, we must consider the following three cases:

- $D = \varepsilon pq$, where $p \neq q$ are odd primes, $\varepsilon \in \{\pm 1\}$, and $\varepsilon pq \equiv 1 \bmod 4$.
- $D = \varepsilon p$, where p is an odd prime, $\varepsilon \in \{\pm 1\}$, and $\varepsilon p \equiv 3 \bmod 4$.
- $D = 2\varepsilon p$, where p is an odd prime and $\varepsilon \in \{\pm 1\}$.

In each of these cases, there are 2 basic genus characters σ, σ', and one of them, say σ, is given by

$$\sigma(F) = \Big(\frac{m}{p}\Big), \quad \text{if the class } F \in \mathfrak{F}_\Delta \text{ represents } m \in \mathbb{Z} \setminus p\mathbb{Z}\,.$$

By Theorem 6.5.12.1, we have $\sigma(F)\sigma'(F) = 1$ for every class $F \in \mathfrak{F}_\Delta$. Hence a class $F \in \mathfrak{F}_\Delta$ lies in the principal genus if and only if $\sigma(F) = 1$. In particular, $4 \,|\, h_\Delta^+$ if and only if A lies in the principal genus, and this holds if and only if $\sigma(f) = 1$ for every non-principal simple ambiguous form of discriminant Δ.

CASE 1: $D = -pq \equiv 1 \bmod 4$, where p and q are distinct odd primes. The only non-principal simple ambiguous form of discriminant $-4pq$ is

$$f = \begin{cases} [p,0,q] & \text{if } p < q\,, \\ [q,0,p] & \text{if } q < p\,, \end{cases} \quad \text{and} \quad \sigma(f) = \Big(\frac{q}{p}\Big) = \Big(\frac{p}{q}\Big) \quad \text{(by quadratic reciprocity).}$$

Hence we obtain

$$4 \,|\, h_{-pq} \quad \text{if and only if} \quad \Big(\frac{q}{p}\Big) = 1\,.$$

CASE 2: $D = -p$ for some prime $p \equiv 1 \bmod 4$. The only non-principal simple ambiguous form of discriminant $-4p$ is

$$f = \Big[2, 2, \frac{p+1}{2}\Big], \quad \text{and} \quad \sigma(f) = \Big(\frac{2}{p}\Big)\,.$$

Hence we obtain

$$4 \,|\, h_{-4p} \quad \text{if and only if} \quad p \equiv 1 \bmod 8\,.$$

CASE 3: $D = -2p$ for some odd prime p. The only non-principal simple ambiguous form of discriminant $-8p$ is

$$f = [2,0,p]\,, \quad \text{and} \quad \sigma(f) = \Big(\frac{2}{p}\Big)\,.$$

Hence we obtain

$$4 \mid h_{-8p} \quad \text{if and only if} \quad p \equiv \pm 1 \bmod 8\,.$$

CASE 4: $D = pq \equiv 1 \bmod 4$, where p and q are distinct odd primes. The three non-principal simple ambiguous forms of discriminant $4pq$ are

$$g = [-1, 0, pq] \quad \text{and} \quad f^{\pm} = \begin{cases} [\pm q, 0, \mp p] & \text{if } q < p\,, \\ [\pm p, 0, \mp q] & \text{if } p < q\,, \end{cases}$$

and it follows that

$$\sigma(g) = \Big(\frac{-1}{p}\Big) \quad \text{and} \quad \sigma(f^{\pm}) = \Big(\frac{\pm q}{p}\Big) \quad \text{or} \quad \Big(\frac{\mp q}{p}\Big)\,, \text{ according as } q < p \text{ or } p < q.$$

Hence we obtain

$$4 \mid h_{4pq} \quad \text{if and only if} \quad p \equiv q \equiv 1 \bmod 4 \quad \text{and} \quad \Big(\frac{p}{q}\Big) = \Big(\frac{q}{p}\Big) = 1\,.$$

CASE 5: $D = p$ for some prime $p \equiv 3 \bmod 4$. Then $g = [-1, 0, p]$ is a simple non-principal ambiguous form of discriminant $4p$, and since $\sigma_1(g) = -1$, we obtain

$$4 \nmid h_{4p}^{+}\,.$$

CASE 6: $D = 2p$ for some odd prime p. The three non-principal simple ambiguous forms of discriminant $8p$ are

$$g = [-1, 0, 2p] \;\text{ and }\; f^{\pm} = [\pm 2, 0, \mp p^{r}]\,, \quad \sigma(g) = \Big(\frac{-1}{p}\Big) \quad \text{and} \quad \sigma(f^{\pm}) = \Big(\frac{\pm 2}{p}\Big)\,.$$

Hence we obtain

$$4 \mid h_{8p}^{+} \quad \text{if and only if} \quad p \equiv 1 \bmod 8\,.$$

For the convenience of the reader and also for later reference, we summarize our results in the subsequent theorem.

Theorem 8.3.5. *Let $\Delta = 4D$ be an even quadratic discriminant such that D is squarefree and the 2-class group $(\mathfrak{F}_\Delta)_2$ is non-trivial and cyclic. Then one of the following cases occurs:*

- $D = -pq \equiv 1 \bmod 4$, *where p and q are distinct odd primes. In this case,*
$$4 \mid h_{-pq} \quad \textit{if and only if} \quad \Big(\frac{q}{p}\Big) = 1\,.$$
- $D = -p$ *for some prime* $p \equiv 1 \bmod 4$. *In this case,*
$$4 \mid h_{-4p} \quad \textit{if and only if} \quad p \equiv 1 \bmod 8\,.$$
- $D = -2p$ *for some odd prime p. In this case,*
$$4 \mid h_{-8p} \quad \textit{if and only if} \quad p \equiv \pm 1 \bmod 8\,.$$
- $D = pq \equiv 1 \bmod 4$, *where p and q are distinct odd primes. In this case,*
$$4 \mid h_{4pq} \quad \textit{if and only if} \quad p \equiv q \equiv 1 \bmod 4 \quad \textit{and} \quad \Big(\frac{p}{q}\Big) = \Big(\frac{q}{p}\Big) = 1\,.$$
- $D = p$ *for some prime* $p \equiv 3 \bmod 4$. *In this case,* $4 \nmid h_{4p}^{+}$.

- $D = 2p$ *for some odd prime* p*. In this case,*

$$4 \mid h_{8p}^{+} \quad \textit{if and only if} \quad p \equiv 1 \mod 8\,.$$

Exercise 8.3.6. Extend Theorem 8.3.5 to arbitrary (not necessarily fundamental) quadratic discriminants.

8.4. Discriminants with cyclic 2-class group: Divisibility by 8 and 16

Let $\Delta = 4D$ be an even quadratic discriminant, where D is squarefree, and assume that the 2-class group $(\mathfrak{F}_\Delta)_2$ is non-trivial and cyclic. In a series of papers, several authors investigated the divisibility of h_Δ^+ by 8 and 16. Among them we mention [**110**], [**52**], [**54**], [**53**], [**69**], [**41**], [**57**], [**68**], [**59**], [**114**], [**55**]. In this section we use a unified approach (based on the results of the previous section) to prove the main criteria for divisibility by 8 and 16.

By Theorem 8.3.5, there is an odd prime p dividing D, and associated with this prime p there is a basic genus character σ such that, for every class $F \in \mathfrak{F}_\Delta$,

$$\sigma(F) = \Big(\frac{m}{p}\Big) \quad \text{if } m \in \mathbb{Z} \setminus p\mathbb{Z} \text{ is represented by } F,$$

and $F \in \mathfrak{F}_\Delta^2$ holds if and only if $\sigma(F) = 1$.

Without further reference, we make extensive use of the results of Chapter 6 and of the elementary properties of the rational biquadratic residue symbol (see Section 7.3). Moreover, we use Corollary A.5.3 for $p = 2$ again and again.

We start with a preliminary technical result for discriminants with two odd prime divisors (Theorem 8.4.1). Once this is proved, the case of negative discriminants follows almost immediately (Theorem 8.4.2), while the case of positive discriminants needs more effort (Theorem 8.4.3).

Theorem 8.4.1. *Let* p *and* q *be distinct primes,* $\delta \in \{\pm 1\}$, $p \equiv \delta q \equiv 1 \mod 4$, $\Delta = 4\delta pq$ *and* $P = [\![p, 0, -\delta q]\!] \in \mathfrak{F}_\Delta$*. Then* $(\mathfrak{F}_\Delta)_2$ *is non-trivial and cyclic, and we denote by* P *the unique non-principal ambiguous class of* $\mathfrak{F}_\Delta$*. Then*

$$P \in \mathfrak{F}_\Delta^2 \quad \textit{if and only if} \quad \Big(\frac{q}{p}\Big) = 1\,.$$

Suppose that $P \in \mathfrak{F}_\Delta^2$*. Then there exist integers* $w \in \mathbb{N}$ *and* $x, y \in \mathbb{Z}$ *such that*

$$(w, 2pq) = (x, y) = 1\,, \quad w^2 = px^2 - \delta qy^2 \quad \textit{and} \quad x \equiv \frac{p+1}{2} \mod 4\,.$$

Whenever integers x, y, w *have these properties, then*

$$\Big(\frac{w}{p}\Big) = \Big[\frac{\delta q}{p}\Big]_4,$$

and we have the following criteria:

$$P \in \mathfrak{F}_\Delta^4 \iff \Big(\frac{w}{p}\Big) = 1\,, \quad \textit{and then} \quad P \in \mathfrak{F}_\Delta^8 \iff \Big[\frac{w}{p}\Big]_4 \Big(\frac{2x}{p}\Big) = 1\,.$$

Proof. As we have seen above, $(\mathfrak{F}_\Delta)_2$ is non-trivial and cyclic, P is the only non-principal ambiguous class, and

$$P \in \mathfrak{F}_\Delta^2 \quad \text{if and only if} \quad \sigma(P) = \Bigl(\frac{q}{p}\Bigr) = 1\,,$$

where σ is the basic genus character associated with p.

Suppose that $P \in \mathfrak{F}_\Delta^2$, say $P = W^2$, where $W \in \mathfrak{F}_\Delta$ and $W = [\![w,*,*]\!]$ for some $w \in \mathbb{N}$ such that $(w, 2pq) = 1$. Then $P = [\![w^2,*,*]\!]$ properly represents w^2, and therefore there exist $x, y \in \mathbb{Z}$ such that $(x,y) = 1$ and $w^2 = px^2 - \delta qy^2$. Since $w^2 \equiv x^2 - y^2 \equiv 1 \bmod 4$, we obtain $2 \nmid x$, and as we may replace x by $-x$, we may assume that

$$x \equiv \frac{p+1}{2} \mod 4\,.$$

From now on let $w \in \mathbb{N}$ and $x, y \in \mathbb{Z}$ be any integers such that

$$(w, 2pq) = (x,y) = 1\,, \quad w^2 = px^2 - \delta qy^2 \quad \text{and} \quad x \equiv \frac{p+1}{2} \mod 4\,.$$

Then P properly represents w^2, hence $P = W^2$ for some $W = [\![w,*,*]\!] \in \mathfrak{F}_\Delta$, and we assert that

$$(*) \qquad \Bigl(\frac{w}{p}\Bigr) = \Bigl[\frac{\delta q}{p}\Bigr]_4\,.$$

Since $w^2 = px^2 - \delta qy^2 \equiv 1 \bmod 8$, it follows that $y = 2^k y_1$, where $y_1 \in \mathbb{Z} \setminus 2\mathbb{Z}$, $k \in \mathbb{N}$, and $k = 1$ if and only if $p \equiv 5 \mod 8$. Since $px^2 \equiv w^2 \mod |y_1|$, we obtain

$$\Bigl(\frac{y}{p}\Bigr) = \Bigl(\frac{2}{p}\Bigr)\Bigl(\frac{y_1}{p}\Bigr) = \Bigl(\frac{2}{p}\Bigr)\Bigl(\frac{p}{|y_1|}\Bigr) = \Bigl(\frac{2}{p}\Bigr) = \Bigl[\frac{-1}{p}\Bigr]_4\,,$$

and

$$\Bigl(\frac{w}{p}\Bigr) = \Bigl[\frac{w^2}{p}\Bigr]_4 = \Bigl[\frac{-\delta qy^2}{p}\Bigr]_4 = \Bigl[\frac{-1}{p}\Bigr]_4\Bigl[\frac{\delta q}{p}\Bigr]_4\Bigl(\frac{y}{p}\Bigr) = \Bigl[\frac{\delta q}{p}\Bigr]_4\,.$$

Hence $(*)$ holds, and we proceed with the criteria for $P \in \mathfrak{F}_\Delta^4$ and $P \in \mathfrak{F}_\Delta^8$.

Obviously, $P \in \mathfrak{F}_\Delta^4$ if and only if $W \in \mathfrak{F}_\Delta^2$, and this holds if and only if

$$\sigma(W) = \Bigl(\frac{w}{p}\Bigr) = 1\,.$$

To obtain the criterion for $P \in \mathfrak{F}_\Delta^8$, we determine explicitly a class $W = [\![w,*,*]\!]$ satisfying $W^2 = P$. Let $\lambda, \mu \in \mathbb{Z}$ be such that $\lambda x - \mu y = 1$. Since we can replace (λ, μ) by $(\lambda + y, \mu + x)$, we may assume that $2 \mid \mu$ and $2 \nmid \lambda$. Now we calculate

$$\begin{pmatrix} x & y \\ \mu & \lambda \end{pmatrix}[p, 0, -\delta q] = [w^2, 2b, c]\,, \quad \text{where} \quad b = px\mu - \delta qy\lambda \ \text{ and } \ c = p\mu^2 - \delta q\lambda^2\,,$$

hence $P = [\![w^2, 2b, c]\!] = [\![w, 2b, cw]\!]^2$, and we assume that $W = [\![w, 2b, cw]\!]$.

Suppose now that $W \in \mathfrak{F}_\Delta^2$, say $W = R^2$, where $R = [\![r,*,*]\!]$ for some $r \in \mathbb{N}$ such that $(r, 2wcpq) = 1$. Since $R^4 = P$, it follows that

$$P \in \mathfrak{F}_\Delta^8 \quad \text{if and only if} \quad \sigma(R) = \Bigl(\frac{r}{p}\Bigr) = 1\,,$$

and therefore it suffices to prove that

$$\Bigl(\frac{r}{p}\Bigr) = \Bigl[\frac{w}{p}\Bigr]_4\Bigl(\frac{2x}{w}\Bigr)\,.$$

Since $W = R^2$ properly represents r^2, there exist $u,\, v \in \mathbb{Z}$ such that

$$(u,v) = 1 \quad \text{and} \quad r^2 = wu^2 + 2buv + cwv^2\,.$$

Replacing (u,v) by $(-u,-v)$ if necessary, we may assume that $k = yu + \lambda vw > 0$, and we set $l = xu + \mu vw$. Then it follows that

$$pl^2 - \delta qk^2 = w^2u^2 + 2buwv + cw^2v^2 = wr^2\,.$$

Now $(r,w) = 1$ implies $(u,w) = 1$, hence $(u,vw) = 1$, and since

$$(l,k) = (u,vw)\begin{pmatrix} x & y \\ \mu & \lambda \end{pmatrix} \quad \text{and} \quad x\lambda - y\mu = 1\,, \text{we obtain} \quad (l,k) = 1\,.$$

Finally, $wr^2 = pl^2 - \delta qk^2$ implies $(l,qwr) = (k,pwr) = 1$.

Now we use the three congruences $wr^2 \equiv -\delta qk^2 \bmod p$, $2buv \equiv r^2 \bmod w$ and $by^2 = -pxy + w^2\lambda y \equiv -pxy \bmod w$ in order to obtain

$$\Big(\frac{p}{w}\Big) = \Big(\frac{w}{p}\Big) = \Big(\frac{-\delta q}{p}\Big) = \Big(\frac{q}{p}\Big) = 1\,,$$

$$1 = \Big(\frac{2buv}{w}\Big) = \Big(\frac{2by^2uv}{w}\Big) = \Big(\frac{-2pxyuv}{w}\Big) \quad \text{and} \quad \Big(\frac{yu}{w}\Big) = \Big(\frac{-2pxv}{w}\Big) = \Big(\frac{-2xv}{w}\Big)\,.$$

Since $wr^2 = pl^2 - \delta qk^2$, it follows that

$$\Big(\frac{r}{p}\Big)\Big[\frac{w}{p}\Big]_4 = \Big[\frac{wr^2}{p}\Big]_4 = \Big[\frac{-1}{p}\Big]_4\Big[\frac{\delta q}{p}\Big]_4\Big(\frac{k}{p}\Big) = \Big(\frac{2}{p}\Big)\Big(\frac{w}{p}\Big)\Big(\frac{k}{p}\Big) = \Big(\frac{2k}{p}\Big)\,,$$

hence

$$\Big(\frac{r}{p}\Big) = \Big[\frac{w}{p}\Big]_4\Big(\frac{2k}{p}\Big)\,, \quad \text{and it remains to prove that} \quad \Big(\frac{2k}{p}\Big) = \Big(\frac{2x}{w}\Big)\,.$$

This is done by a calculation of Jacobi symbols in various cases.

CASE 1: $w \equiv 1 \bmod 4$. Since $wr^2 = pl^2 - \delta qk^2 \equiv 1 \bmod 4$, we obtain $2 \nmid l$, $2 \,|\, k$, and $k \equiv 2 \bmod 4$ if and only if $p \not\equiv w \bmod 8$. Since $2 \,|\, y$ and $2 \nmid \lambda w$, it follows that $2 \,|\, v$, and as $2 \nmid u\lambda w$, we get $k = yu + \lambda wv \equiv y + v \bmod 4$. We set $k = 2^\tau k_1$ and $v = 2^\omega v_1$, where $k_1,\, \tau,\, \omega \in \mathbb{N}$, $v_1 \in \mathbb{Z}$ and $2 \nmid k_1v_1$. Finally, we use the congruences $pl^2 \equiv wr^2 \bmod k_1$, $k \equiv yu \bmod w$ and $wu^2 \equiv r^2 \bmod |v_1|$ to perform the following calculations of Jacobi symbols.

$$\Big(\frac{v}{w}\Big) = \Big(\frac{2}{w}\Big)^{\omega}\Big(\frac{v_1}{w}\Big) = \Big(\frac{2}{w}\Big)^{\omega}\Big(\frac{w}{|v_1|}\Big) = \Big(\frac{2}{w}\Big)^{\omega}$$

and

$$\begin{aligned}\Big(\frac{2k}{p}\Big) &= \Big(\frac{2}{p}\Big)^{\tau+1}\Big(\frac{k_1}{p}\Big) = \Big(\frac{2}{p}\Big)^{\tau+1}\Big(\frac{p}{k_1}\Big) = \Big(\frac{2}{p}\Big)^{\tau+1}\Big(\frac{w}{k_1}\Big) = \Big(\frac{2}{p}\Big)^{\tau+1}\Big(\frac{k_1}{w}\Big) \\ &= \Big(\frac{2}{p}\Big)^{\tau+1}\Big(\frac{2}{w}\Big)^{\tau}\Big(\frac{k}{w}\Big) = \Big(\frac{2}{p}\Big)^{\tau+1}\Big(\frac{2}{w}\Big)^{\tau}\Big(\frac{yu}{w}\Big) = \Big(\frac{2}{p}\Big)^{\tau+1}\Big(\frac{2}{w}\Big)^{\tau}\Big(\frac{-2xv}{w}\Big) \\ &= \Big(\frac{2}{p}\Big)^{\tau+1}\Big(\frac{2}{w}\Big)^{\tau+1}\Big(\frac{v}{w}\Big)\Big(\frac{x}{w}\Big) = \Big(\frac{2}{p}\Big)^{\tau+1}\Big(\frac{2}{w}\Big)^{\omega+\tau+1}\Big(\frac{x}{w}\Big)\,.\end{aligned}$$

- If $p \equiv w \equiv 1 \bmod 8$, then
$$\Big(\frac{2k}{p}\Big) = \Big(\frac{x}{w}\Big) = \Big(\frac{2x}{w}\Big)\,.$$
- If $p \equiv 1 \bmod 8$ and $w \equiv 5 \bmod 8$, then $k \equiv 2 \bmod 4$, $y \equiv 0 \bmod 4$, and therefore $v \equiv 2 \bmod 4$. Hence $\tau = \omega = 1$, and
$$\Big(\frac{2k}{p}\Big) = \Big(\frac{2}{w}\Big)\Big(\frac{x}{w}\Big) = \Big(\frac{2x}{w}\Big)\,.$$
- If $p \equiv 5 \bmod 8$ and $w \equiv 1 \bmod 8$, then $k \equiv 2 \bmod 4$, hence $\tau = 1$, and
$$\Big(\frac{2k}{p}\Big) = \Big(\frac{x}{w}\Big) = \Big(\frac{2x}{w}\Big)\,.$$
- If $p \equiv w \equiv 5 \bmod 8$, then $k \equiv 0 \bmod 4$, $y \equiv 2 \bmod 4$, hence $v \equiv 2 \bmod 4$, $\omega = 1$, and we obtain
$$\Big(\frac{2k}{p}\Big) = (-1)^{\tau+1}(-1)^{\tau+2}\Big(\frac{x}{w}\Big) = -\Big(\frac{x}{w}\Big) = \Big(\frac{2}{w}\Big)\Big(\frac{x}{w}\Big) = \Big(\frac{2x}{w}\Big)\,.$$

CASE 2: $w \equiv 3 \bmod 4$. Since $wr^2 = pl^2 - \delta qk^2 \equiv 3 \bmod 4$, we obtain $2 \,|\, l$, $2 \nmid k$, and $2 \,|\, y$ implies $2 \nmid v$. Since $l = xu + \mu vw \equiv xu \equiv 0 \bmod 2$, we obtain $2 \,|\, u$, hence $4 \,|\, uy$, and therefore $k \equiv \lambda wv \equiv -\lambda v \bmod 4$. Since $4 \,|\, \mu y$, it follows that $\lambda x = 1 + \mu y \equiv 1 \bmod 4$ and $kv \equiv -\lambda v^2 \equiv -\lambda \equiv -x \bmod 4$. Finally, using the congruences $pl^2 \equiv wr^2 \bmod k$, $k \equiv yu \bmod w$ and $wu^2 \equiv r^2 \bmod |v|$, we get
$$\Big(\frac{v}{w}\Big)) = \Big(\frac{w}{|v|}\Big)(-1)^{(v-1)/2} = (-1)^{(v-1)/2}$$
and
$$\begin{aligned}\Big(\frac{2k}{p}\Big) &= \Big(\frac{2}{p}\Big)\Big(\frac{p}{k}\Big) = \Big(\frac{2}{p}\Big)\Big(\frac{w}{k}\Big) = \Big(\frac{2}{p}\Big)\Big(\frac{k}{w}\Big)(-1)^{(k-1)/2} = \Big(\frac{2}{p}\Big)\Big(\frac{yu}{w}\Big)(-1)^{(k-1)/2} \\ &= \Big(\frac{2}{p}\Big)\Big(\frac{-2xv}{w}\Big)(-1)^{(k-1)/2} = -\Big(\frac{2}{p}\Big)\Big(\frac{2x}{w}\Big)\Big(\frac{v}{w}\Big)(-1)^{(k-1)/2} \\ &= \Big(\frac{2x}{w}\Big)(-1)^{1+(p-1)/4+(v-1)/2+(k-1)/2} = \Big(\frac{2x}{w}\Big)\,,\end{aligned}$$
since
$$1 + \frac{v-1}{2} + \frac{k-1}{2} = \frac{v+k}{2} \equiv \frac{-kv-1}{2} \equiv \frac{x-1}{2} \equiv \frac{\frac{p+1}{2}-1}{2} \equiv \frac{p-1}{4} \mod 2\,. \qquad \square$$

Theorem 8.4.2. *Let p and q be primes such that*
$$p \equiv -q \equiv 1 \bmod 4 \quad \textit{and} \quad \Big(\frac{q}{p}\Big) = 1\,.$$
Then
$$4 \,|\, h_{-4pq}\,, \quad \Big(\frac{w}{p}\Big) = \Big[\frac{-q}{p}\Big]_4, \quad \textit{and} \quad 8 \,|\, h_{-4pq} \ \textit{ if and only if } \ \Big[\frac{-q}{p}\Big]_4 = 1\,.$$
Suppose that $8 \,|\, h_{-4pq}$. Then there exist $w \in \mathbb{N}$ and $x,\, y \in \mathbb{Z}$ such that
$$(w, 2pq) = (x, y) = 1\,, \quad w^2 = px^2 + qy^2 \quad \textit{and} \quad x \equiv \frac{p+1}{2} \mod 4\,.$$

Whenever integers x, y, w have these properties, then

$$16 \mid h_{-4pq} \quad \textit{if and only if} \quad \Big[\frac{w}{p}\Big]_4 \Big(\frac{2x}{p}\Big) = 1\,.$$

Proof. Apart from the principal form, there is only one simple ambiguous form of discriminant $-4pq$, namely $[p,0,q]$ if $p<q$, and $[q,0,p]$ if $q<p$. Therefore the class $P = [\![p,0,q]\!] = [\![q,0,p]\!] \in \mathfrak{F}_{-4pq}$ has order 2, and for any $n \in \mathbb{N}$, we obtain $2^{n+1} \mid h_{-4pq}$ if and only if $P \in \mathfrak{F}_{-4pq}^{2^n}$. Hence the result follows by Theorem 8.4.1, applied with $\delta = -1$. □

Theorem 8.4.3. *Let p and q be distinct primes such that*

$$p \equiv q \equiv 1 \bmod 4\,, \quad p = a^2+b^2, \quad q = c^2+d^2 \quad \textit{and} \quad \Big(\frac{p}{q}\Big) = 1\,,$$

where a, b, c, $d \in \mathbb{N}$, and $2 \nmid ac$. Then $4 \mid h_{4pq}^+$.

1. *There exists exactly one $\sigma \in \{-1, p, q\}$ such that the Diophantine equation $x^2 - pqy^2 = \sigma$ is solvable. If $H = [\![1,0,-pq]\!] \in \mathfrak{F}_{4pq}$ denotes the principal class, then*
   - *$\sigma = -1$ [hence $\mathcal{N}(\varepsilon_{4pq}) = -1$] if and only if $H = [\![-1,0,pq]\!]$,*
   - *$\sigma = p$ if and only if $H = [\![p,0,-q]\!]$,*
   - *$\sigma = q$ if and only if $H = [\![q,0,-p]\!]$.*
2. *Let $\sigma \in \{-1, p, q\}$ be such that the Diophantine equation $x^2 - pqy^2 = \sigma$ is solvable.*
   (a) *If $\sigma = -1$, then*

   $$\Big[\frac{p}{q}\Big]_4 = \Big[\frac{q}{p}\Big]_4 = (-1)^{h_{4pq}^+/4} \quad \textit{and} \quad \Big(\frac{ac+bd}{p}\Big) = 1\,.$$

   (b) *$\sigma = p$ if and only if there exist u, $v \in \mathbb{N}$ such that $pu^2 - qv^2 = 1$. In this case, it follows that*

   $$\Big[\frac{p}{q}\Big]_4 = 1 \quad \textit{and} \quad \Big[\frac{q}{p}\Big]_4 = \Big(\frac{ac+bd}{p}\Big) = (-1)^{h_{4pq}^+/4}\,.$$

   (c) *$\sigma = q$ if and only if there exist u, $v \in \mathbb{N}$ such that $pu^2 - qv^2 = -1$. In this case, it follows that*

   $$\Big[\frac{q}{p}\Big]_4 = 1 \quad \textit{and} \quad \Big[\frac{p}{q}\Big]_4 = \Big(\frac{ac+bd}{p}\Big) = (-1)^{h_{4pq}^+/4}\,.$$

3. *We have*

$$\mathcal{N}(\varepsilon_{4pq}) = -1 \quad \textit{if and only if} \quad \Big[\frac{p}{q}\Big]_4 = \Big[\frac{q}{p}\Big]_4 = -1$$

and

$$8 \mid h_{4pq}^+ \quad \textit{if and only if} \quad \Big[\frac{p}{q}\Big]_4 = \Big[\frac{q}{p}\Big]_4 = 1\,.$$

4. *Suppose that* $8 \mid h_{4pq}^+$. *Then there exist* $w,\, w_1 \in \mathbb{N}$ *and* $x,\, y,\, x_1,\, y_1 \in \mathbb{Z}$ *such that* $(x,y) = (x_1,y_1) = (ww_1, 2pq) = 1$, $w^2 = px^2 - qy^2$, $w_1^2 = qx_1^2 - py_1^2$

$$\Big(\frac{w}{p}\Big) = \Big(\frac{w_1}{q}\Big) = 1\,, \quad x \equiv \frac{p+1}{2} \mod 4 \quad \textit{and} \quad x_1 \equiv \frac{q+1}{2} \mod 4\,.$$

Whenever integers x, y, x_1, y_1 *and* w, w_1 *have these properties, then*

$$16 \mid h_{4pq}^+ \quad \textit{if and only if} \quad \Big[\frac{w}{p}\Big]_4 \Big(\frac{2x}{w}\Big) = \Big[\frac{w_1}{q}\Big]_4 \Big(\frac{2x_1}{w_1}\Big) = 1\,.$$

Proof. Note that $4 \mid h_{4pq}^+$ follows by Theorem 8.3.5.

1. There are three non-principal simple ambiguous forms of discriminant $4pq$, namely $g = [-1, 0, pq]$, and $f^\pm = [\pm p, 0, \mp q]$ or $f^\pm = [\pm q, 0, \mp p]$, depending on whether $p < q$ or $q < p$. We set

$$M = [\![-1, 0, pq]\!]\,, \quad P = [\![p, 0, -q]\!] = [\![-q, 0, p]\!] \ \text{ and } \ Q = [\![q, 0, -p]\!] = [\![-p, 0, q]\!]\,,$$

and we denote by $A \in \mathfrak{F}_{4pq}$ the non-principal ambiguous class. Then it follows that $\{H, A\} = \{M, P, Q\} = \{\, [\![g]\!],\, [\![f^\pm]\!]\}$, and precisely one of the classes M, P, Q equals H. Therefore H represents

- -1 if $M = H$ and $P = Q \neq H$;
- p if $P = H$ and $M = Q \neq H$;
- q if $Q = H$ and $M = P \neq H$.

2. We maintain the notation from 1. Since $pq = (ac+bd)^2 + (ad-bc)^2$ and $(ac+bd, 2(ad-bc)) = 1$, get $J = [\![ac+bd, 2(ad-bc), -(ac+bd)]\!] \in \mathfrak{F}_{4pq}$, and $J^2 = [\![(ac+bd)^2, 2(ad-bc), -1]\!] = M$. By Theorem 8.4.1 it follows that

$$P \in \mathfrak{F}_{4pq}^4 \ \text{ if and only if } \ \Big[\frac{q}{p}\Big]_4 = 1\,, \quad \text{and} \quad Q \in \mathfrak{F}_{4pq}^4 \ \text{ if and only if } \ \Big[\frac{p}{q}\Big]_4 = 1\,.$$

Now we can finish the proof. Since the assertions are symmetric in p and q, we may assume that either $M = H$ or $P = H$.

CASE 1: $M = H$. Then $\sigma = -1$, $P = Q \neq H$, $J \in \mathfrak{F}_{4pq}^2$, and $P = Q \in \mathfrak{F}_{4pq}^4$ if and only if $8 \mid h_{4pq}^+$. Hence it follows that

$$\Big[\frac{p}{q}\Big]_4 = \Big[\frac{q}{p}\Big]_4 = (-1)^{h_{4pq}^+/4} \quad \text{and} \quad \Big(\frac{ac+bd}{p}\Big) = 1\,.$$

CASE 2: $P = H$. Then $J^2 = M = Q \neq H$, $P \in \mathfrak{F}_{4pq}^4$, and $J^2 = Q \in \mathfrak{F}_{4pq}^4$ if and only if $8 \mid h_{4pq}^+$. Hence

$$\Big(\frac{ad+bc}{p}\Big) = \Big[\frac{p}{q}\Big]_4 = (-1)^{h_{4pq}^+/4} \quad \text{and} \quad \Big[\frac{p}{q}\Big]_4 = 1\,.$$

3. Obvious by 2.

4. Note that either $P = H$ and $Q \neq H$, or $Q = H$ and $P \neq H$. Hence $16 \mid h_{4pq}^+$ if and only if both P and Q are eighth powers, and the assertion follows by Theorem 8.4.1. ☐

Exercise 8.4.4. Let p and q be distinct primes such that $p \equiv q \equiv 1 \bmod 4$, $p < q$,

$$\Big(\frac{p}{q}\Big) = 1\,, \quad \mathcal{N}(\varepsilon_{4pq}) = 1\,, \quad \text{and let } 2k \text{ be the period length of } \sqrt{pq}.$$

Prove that the Diophantine equation $x^2 - pqy^2 = (-1)^k p$ is solvable. Hint: Use Exercise 5.7.10.

Exercise 8.4.5. Deduce Burde's reciprocity law (Theorem 7.5.3 for primes) from Theorem 8.4.3.

Theorem 8.4.6. *Let $p \equiv 1 \bmod 8$ be a prime, and let $a,\, b,\, s,\, t \in \mathbb{N}$ be such that $4\,|\,b$ and $p = a^2 + b^2 = 2s^2 - t^2$* (see Theorem 6.2.6.3). *Then $2 \nmid st$ and $4\,|\,h_{-4p}$.*

1. $8\,|\,h_{-4p}$ *if and only if one of the following equivalent conditions is fulfilled*:

$$\text{(a)} \quad a + b \equiv \pm 1 \mod 8\,; \qquad \text{(b)} \quad \Big(\frac{s}{p}\Big) = 1\,; \qquad \text{(c)} \quad s \equiv 1 \mod 4\,.$$

2. *Suppose that $8\,|\,h_{-4p}$. Then*

$$16\,|\,h_{-4p} \quad \textit{if and only if} \quad \Big[\frac{s}{p}\Big]_4 = \Big(\frac{2t}{s}\Big)\,.$$

Proof. Note that $2 \nmid st$ since $p \equiv 1$ mod 8, and $4\,|\,h_{-4p}$ by Theorem 8.3.5.

1. The equivalence of (a), (b) and (c) follows, since

$$\Big(\frac{2}{a+b}\Big) = \Big(\frac{s}{p}\Big) = (-1)^{(s-1)/2}$$

by Theorem 6.2.6.4(a).

The form $f = [2, 2, (p+1)/2]$ is the only non-principal simple ambiguous form of discriminant $-4p$. Therefore $A = [\![f]\!]$ is the only non-principal ambiguous class and represents 2. Since $J = [\![s, 2t, 2s]\!] \in \mathcal{F}_{-4p}$ and $J^2 = [\![s^2, 2t, 2]\!]$ represents 2, it follows by Theorem 6.4.13.2 that $J^2 = A$. Consequently, $\mathrm{ord}(J) = 4$, and $8\,|\,h_{-4p}$ if and only if J is a square, which is equivalent to

$$\sigma(J) = \Big(\frac{s}{p}\Big) = 1\,.$$

2. Since $8\,|\,h_{-4p}$, it follows that $J = R^2$ for some class $R \in \mathfrak{F}_{-4p}$, and we may assume that $R = [\![r, *, *]\!]$ for some $r \in \mathbb{N}$ such that $(r, 2ps) = 1$. Then $16\,|\,h_{-4p}$ if and only if R is a square, that is, if and only if

$$\sigma(R) = \Big(\frac{r}{p}\Big) = 1\,, \quad \text{and we must prove that} \quad \Big(\frac{r}{p}\Big) = \Big[\frac{s}{p}\Big]_4 \Big(\frac{2t}{s}\Big)\,.$$

Since J properly represents r^2, there exist $u,\, v \in \mathbb{Z}$ such that $(u, v) = 1$ and $r^2 = su^2 + 2tuv + 2sv^2$. Replacing (u, v) by $(-u, -v)$ if necessary, we may assume that $k = tu + 2sv > 0$, and we obtain

$$2sr^2 = k^2 + pu^2\,.$$

We assert that $(k, 2p) = (u, r) = (u, s) = (u, k) = (k, s) = 1$. Indeed, since $2 \nmid u$, it follows that $2 \nmid k$, and therefore $(p, 2rs) = 1$ implies $(k, 2p) = 1$. Next, as $(u, r) \,|\, 2sv^2$ and $(r, 2s) = (u, v) = 1$, it follows that $(u, r) = 1$, and consequently also $(u, s) = 1$. Since $(u, k) \,|\, 2rs$ and $u, 2s) = (u, r) = 1$, we obtain $(u, k) = 1$. Finally, $(k, s) \,|\, pu^2$ implies $(k, s) = 1$.

From the congruence $k^2 - 1 = 2sr^2 - (2s^2 - t^2)u^2 - 1 \equiv 2s - 2 + t^2u^2 - 1 \bmod 16$ we obtain

$$\frac{k^2-1}{8} \equiv \frac{s-1}{4} + \frac{t^2u^2-1}{8} \bmod 2 \qquad \text{and} \qquad \Big(\frac{2}{k}\Big) = \Big(\frac{2}{s}\Big)\Big(\frac{2}{t|u|}\Big) = \Big(\frac{2}{st|u|}\Big).$$

Next, observe that $k^2 \equiv 2sr^2 \bmod p|u|$, $pu^2 \equiv 2sl^2 \bmod k$, $k \equiv tu \bmod s$, and

$$\Big[\frac{2}{p}\Big]_4 = (-1)^{b/4} = \Big(\frac{2}{t}\Big) \qquad \text{(by the Theorems 7.5.1.2(a) and 6.2.6.4).}$$

Then we obtain

$$\Big(\frac{k}{p}\Big) = \Big[\frac{k^2}{p}\Big]_4 = \Big[\frac{2sr^2}{p}\Big]_4 = \Big[\frac{2}{p}\Big]_4\Big[\frac{s}{p}\Big]_4\Big(\frac{r}{p}\Big) = \Big(\frac{2}{t}\Big)\Big[\frac{s}{p}\Big]_4\Big(\frac{r}{p}\Big),$$

hence

$$\Big(\frac{r}{p}\Big) = \Big[\frac{s}{p}\Big]_4\Big(\frac{k}{p}\Big)\Big(\frac{2}{t}\Big), \quad \text{and we must prove that} \quad \Big(\frac{k}{p}\Big)\Big(\frac{2}{t}\Big) = \Big(\frac{2t}{s}\Big).$$

By repeated application of the quadratic reciprocity, we finally get

$$\begin{aligned}\Big(\frac{k}{p}\Big)\Big(\frac{2}{t}\Big) &= \Big(\frac{p}{k}\Big)\Big(\frac{2}{t}\Big) = \Big(\frac{2s}{k}\Big)\Big(\frac{2}{t}\Big) = \Big(\frac{2}{st|u|}\Big)\Big(\frac{s}{k}\Big)\Big(\frac{2}{t}\Big) = \Big(\frac{2}{s|u|}\Big)\Big(\frac{k}{s}\Big) \\ &= \Big(\frac{2}{s|u|}\Big)\Big(\frac{tu}{s}\Big) = \Big(\frac{2}{s|u|}\Big)\Big(\frac{t}{s}\Big)\Big(\frac{s}{|u|}\Big) = \Big(\frac{2}{s|u|}\Big)\Big(\frac{t}{s}\Big)\Big(\frac{2}{|u|}\Big) = \Big(\frac{2t}{s}\Big). \quad \Box\end{aligned}$$

Theorem 8.4.7. *Let* $p \equiv \pm 1 \bmod 8$ *be a prime and let* $e, f \in \mathbb{N}$ *be such that* $e \equiv 1 \bmod 4$ *and* $p = e^2 - 2f^2$ (see Theorem 6.2.6). *Then* $4 \,|\, h_{-8p}$.

A. *Suppose that* $p \equiv 1 \bmod 8$ *and* $p = a^2 + b^2$, *where* $a, b \in \mathbb{N}$ *and* $4 \,|\, b$.

1. $8 \,|\, h_{-8p}$ *if and only if one of the following equivalent conditions is fulfilled*:

$$\text{(a)} \quad \Big(\frac{e}{p}\Big) = 1; \qquad \text{(b)} \quad e \equiv 1 \bmod 8; \qquad \text{(c)} \quad b \equiv 0 \bmod 8.$$

2. *Suppose that* $8 \,|\, h_{-8p}$. *Then*

$$16 \,|\, h_{-8p} \quad \textit{if and only if} \quad \Big[\frac{e}{p}\Big]_4 = 1.$$

B. *Suppose that* $p \equiv -1 \bmod 8$.

1. $8 \,|\, h_{-8p}$ *if and only if one of the following equivalent conditions is fulfilled*:

$$\text{(a)} \quad \Big(\frac{e}{p}\Big) = 1; \qquad \text{(b)} \quad e \equiv 1 \bmod 8; \qquad \text{(c)} \quad p \equiv -1 \bmod 16.$$

2. *Suppose that* $8 \,|\, h_{-8p}$. *Then*

$$16 \,|\, h_{-8p} \quad \textit{if and only if} \quad (-1)^{(e-1)/8}\Big(\frac{e}{f}\Big) = 1.$$

Proof. Note that $f \equiv 0 \bmod 2$ if $p \equiv 1 \bmod 8$, $f \equiv 1 \bmod 2$ if $p \equiv -1 \bmod 8$, and $4 \,|\, h_{-8p}$ by Theorem 8.3.5. We prove **A** and **B** by concurrent arguments.

1. In both cases, the equivalence of (a) and (b) follows since

$$(-1)^{(e-1)/4} = \Big(\frac{-2}{e}\Big) = \Big(\frac{p}{e}\Big) = \Big(\frac{e}{p}\Big) = (-1)^{b/4}\,,$$

observing that $e \equiv 1 \bmod 4$. The equivalence of (a) and (c) in **A** follows since

$$\Big(\frac{e}{p}\Big) = (-1)^{b/4} \quad \text{by Theorem 6.2.6.4(a)}\,,$$

and the equivalence of (b) and (c) in **B** follows since $p \equiv -1 \bmod 8$ implies $2 \nmid f$ and therefore $p \equiv e^2 - 2 \bmod 16$.

The form $[2, 0, p]$ is the only non-principal simple ambiguous form of discriminant $-8p$. Therefore $A = [\![2, 0, p]\!]$ is the only non-principal ambiguous class and represents 2. Since $J = [\![e, 4f, 2e]\!] \in \mathfrak{F}_{-8p}$ and $J^2 = [\![e^2, 4f, 2]\!]$ represents 2, it follows by Theorem 6.4.13.2 that $J^2 = A$. Consequently, $\mathrm{ord}(J) = 4$, and $8 \,|\, h_{-8p}$ if and only if J is a square, which is equivalent to

$$\sigma(J) = \Big(\frac{e}{p}\Big) = 1\,.$$

2. Suppose that $8 \,|\, h_{-8p}$ and the conditions (a), (b) and (c) hold. Then $J = R^2$ for some class $R \in \mathfrak{F}_{-8p}$, and we may assume that $R = [\![r, *, *]\!]$, where $r \in \mathbb{N}$ and $(r, 2pe) = 1$. Hence it follows that $16 \,|\, h_{-4p}$ if and only if R is a square, that is, if and only if

$$\sigma(R) = \Big(\frac{r}{p}\Big) = 1\,.$$

Since J properly represents r^2, there exist $u, v \in \mathbb{Z}$ such that $(u, v) = 1$ and $r^2 = eu^2 + 4fuv + 2ev^2$. We set $k = ev + fu$ and obtain

$$er^2 = 2k^2 + pu^2 \equiv 1 \bmod 8\,.$$

CASE **A.** $p \equiv 1 \bmod 8$. We must prove that

$$\Big(\frac{r}{p}\Big) = \Big[\frac{e}{p}\Big]_4\,.$$

Since $2k^2 + pu^2 \equiv 1 \bmod 8$, it follows that $k = 2^\tau k_1$, where $\tau \in \mathbb{N}$, $k_1 \in \mathbb{Z} \setminus 2\mathbb{Z}$, and $k \equiv u + v \equiv 0 \bmod 2$ implies $2 \nmid uv$.

For the following calculation of Jacobi symbols, we observe that $e \equiv 1 \bmod 8$,

$$\Big[\frac{2}{p}\Big]_4 = (-1)^{b/4} = 1\,,$$

$$pu^2 \equiv er^2 \bmod |k_1|\,, \quad k \equiv fu \bmod e\,, \quad 4fuv \equiv r^2 \bmod e\,, \quad eu^2 \equiv r^2 \bmod |v|$$

and $(er, p) = (k, p) = (e, k) = (e, u) = (e, v) = 1$. Then we obtain

$$\begin{aligned}\Big[\frac{e}{p}\Big]_4\Big(\frac{r}{p}\Big) &= \Big[\frac{er^2}{p}\Big]_4 = \Big[\frac{2k^2}{p}\Big]_4 = \Big[\frac{2}{p}\Big]_4\Big(\frac{k}{p}\Big) = \Big(\frac{k_1}{p}\Big) = \Big(\frac{p}{|k_1|}\Big) = \Big(\frac{e}{|k_1|}\Big) = \Big(\frac{k_1}{e}\Big) \\ &= \Big(\frac{k}{e}\Big) = \Big(\frac{fu}{e}\Big) = \Big(\frac{v}{e}\Big) = \Big(\frac{e}{|v|}\Big) = 1\,, \quad \text{and consequently} \quad \Big[\frac{e}{p}\Big]_4 = \Big(\frac{r}{p}\Big)\,.\end{aligned}$$

CASE **B.** $p \equiv -1 \bmod 8$. We must prove that

$$\Big(\frac{r}{p}\Big) = (-1)^{(e-1)/8)}\Big(\frac{f}{e}\Big), \quad \text{and we observe that} \quad \Big(\frac{r}{p}\Big) = \Big(\frac{2}{r}\Big) = (-1)^{(r^2-1)/8}$$

by Theorem 6.5.12.

Since $2k^2+pu^2 \equiv 1 \bmod 8$, it follows that $2 \nmid k$, and therefore

$$er^2-1 = 2k^2+(e^2-2f^2)u^2-1 \equiv 2+e^2u^2-2-1 \equiv e^2u^2-1 \bmod 16\,.$$

We observe the congruences

$$e \equiv 1 \bmod 8\,, \quad 2k^2 \equiv er^2 \bmod |u|\,, \quad 4fuv \equiv r^2 \bmod e \quad \text{and} \quad eu^2 \equiv r^2 \bmod |v|$$

and obtain

$$\begin{aligned}(-1)^{(e-1)/8}(-1)^{(r^2-1)/8} &= (-1)^{(er^2-1)/8} = (-1)^{(e^2u^2-1)/8} = \Big(\frac{2}{e|u|}\Big) = \Big(\frac{2}{e}\Big)\Big(\frac{2}{|u|}\Big) \\ &= \Big(\frac{2}{|u|}\Big) = \Big(\frac{e}{|u|}\Big) = \Big(\frac{u}{e}\Big) = \Big(\frac{fv}{e}\Big) = \Big(\frac{f}{e}\Big)\Big(\frac{e}{|v|}\Big) = \Big(\frac{f}{e}\Big)\,.\end{aligned}$$

Hence the assertion follows. □

Theorem 8.4.8. *Let* $p \equiv 1 \bmod 8$ *be a prime. Then* $4 \mid h_{8p}^+$.

1. *There exists exactly one* $\sigma \in \{-1, 2, -2\}$ *such that the Diophantine equation* $x^2-2py^2=\sigma$ *is solvable. If* $H = [\![1,0,-2p]\!] \in \mathfrak{F}_{8p}$ *denotes the principal class, then*
   - $\sigma = -1$ *[hence* $\mathcal{N}(\varepsilon_{2p}) = -1$*] if and only if* $H = [\![-1,0,2p]\!]$.
   - $\sigma = \pm 2$ *if and only if* $H = [\![\pm 2, 0, \mp p]\!]$.

   If $\mathcal{N}(\varepsilon_{2p}) = 1$ *and* $2k$ *is the period length of* $\sqrt{2p}$, *then* $\sigma = 2(-1)^k$.
2. *Let* $a, b, c, d, s, t \in \mathbb{N}$ *such that*

   $$p = a^2+b^2 = c^2+2d^2 = 2s^2-t^2 \quad \textit{and} \quad 4 \mid b \quad (\text{see Theorem } 6.2.6)\,.$$

   Then $8 \mid h_{8p}^+$ *if and only if one of the following equivalent conditions is fulfilled:*
   - (a) $\Big(\dfrac{c}{p}\Big) = \Big(\dfrac{t}{p}\Big) = 1$;
   - (b) $\Big(\dfrac{2}{c}\Big) = \Big(\dfrac{2}{t}\Big) = 1$;
   - (c) $a \equiv \pm 1 \bmod 8$ *and* $b \equiv 0 \bmod 8$;
   - (d) $p \equiv 1 \bmod 16$ *and* $\Big[\dfrac{2}{p}\Big]_4 = 1$;
   - (e) $t \equiv \pm 1 \bmod 8$ *and* $\Big(\dfrac{s}{p}\Big) = 1$;
   - (f) $d \equiv 0 \bmod 4$ *and* $\Big(\dfrac{c}{p}\Big) = 1$.

3. *Suppose that* $8\,|\,h_{2p}^+$. *Then there exist* $c,\ d,\ s,\ t\in\mathbb{N}$ *such that*

$$t\equiv 1 \bmod 8\,,\quad \Bigl(\frac{c}{p}\Bigr)=1 \quad \textit{and}\quad p=c^2+2d^2=2s^2-t^2\,.$$

Whenever integers $c,\ d,\ s,\ t$ *have these properties, then*

$$16\,|\,h_{8p}^+ \quad \textit{if and only if}\quad \Bigl[\frac{c}{p}\Bigr]_4=(-1)^{(t-1)/8}\Bigl(\frac{s}{t}\Bigr)=1\,.$$

Proof. Note that $4\,|\,h_{8p}^+$ by Theorem 8.3.5.

1. There are three non-principal simple ambiguous forms of discriminant $8p$, namely $g=[-1,0,2p]$ and $f^\pm=[\pm2,0,\mp p]$. We set

$$M=[\![-1,0,2p]\!]\,,\quad P=[\![p,0,-2]\!]=[\![-2,0,p]\!] \ \text{ and }\ Q=[\![2,0,-p]\!]=[\![-p,0,2]\!]\,,$$

and we denote by $A\in\mathfrak{F}_{8p}$ the non-principal ambiguous class. then it follows that $\{H,A\}=\{M,P,Q\}=\{\,[\![g]\!],\ [\![f^\pm]\!]\}$, precisely one of the classes M, P, Q equals H, and the other two equal A. Therefore H represents

- -1 if $M=H$ and $P=Q\neq H$;
- p if $P=H$ and $M=Q\neq H$;
- 2 if $Q=H$ and $M=P\neq H$.

Moreover, if $n\in\mathbb{N}$, then $2^{n+1}\,|\,h_{8p}^+$ if and only if P and Q are both 2^n-th powers.

If $\mathcal{N}(\varepsilon_{2p})=1$ and $2k$ is the period length of $\sqrt{2p}$, then the Diophantine equation $2x^2-py^2=(-1)^k$ is solvable by Theorem 5.7.7. However, this holds if and only if the Diophantine equation $x^2-2py^2=2(-1)^k$ is solvable, that is, if and only if $\sigma=(-1)^k$.

2. We prove first the equivalence of the conditions (a) to (e) using the Theorems 6.2.6.4 and 7.5.1.2(b).

(a) $\Leftrightarrow$ (b) Since $p=c^2+2d^2=2s^2-t^2$, it follows that

$$\Bigl(\frac{c}{p}\Bigr)=\Bigl(\frac{p}{c}\Bigr)=\Bigl(\frac{2}{c}\Bigr)\quad\text{and}\quad\Bigl(\frac{t}{p}\Bigr)=\Bigl(\frac{p}{t}\Bigr)=\Bigl(\frac{2}{t}\Bigr)\,.$$

(b) $\Rightarrow$ (c) This holds, since

$$\Bigl(\frac{2}{t}\Bigr)=\Bigl(\frac{2}{a}\Bigr)\quad\text{and}\quad\Bigl(\frac{2}{c}\Bigr)=(-1)^{b/8}\,.$$

(c) $\Rightarrow$ (d) Obviously, (b) implies $p\equiv1 \bmod 16$, and

$$\Bigl[\frac{2}{p}\Bigr]_4=(-1)^{b/4}\,.$$

(d) $\Rightarrow$ (e) Clearly, $2\nmid st$, hence $2s^2\equiv2 \bmod 16$ and $t^2=2s^2-p\equiv1 \bmod 16$. Therefore we obtain $t\equiv\pm1 \bmod 8$, and

$$\Bigl(\frac{s}{p}\Bigr)=\Bigl(\frac{2}{t}\Bigr)(-1)^{b/4}=\Bigl(\frac{2}{t}\Bigr)\Bigl[\frac{2}{p}\Bigr]_4=1\,.$$

(e) $\Rightarrow$ (f) As $s\equiv1 \bmod 2$ and $t\equiv\pm1 \bmod 8$, we get $p=2s^2-t^2\equiv1 \bmod 16$,

$$1=\Bigl(\frac{s}{p}\Bigr)=\Bigl(\frac{2}{t}\Bigr)(-1)^{b/4}=(-1)^{b/4}=(-1)^{(p-1)/8+d/2}=(-1)^{d/2},$$

and therefore $d\equiv0 \bmod 4$.

(f) $\Rightarrow$ (b) Since

$$1=\Big(\frac{c}{p}\Big)=\Big(\frac{2}{c}\Big)=(-1)^{b/4}\,,\quad \text{we get}\quad b\equiv 0 \bmod 8 \ \text{ and } \ c\equiv \pm 1 \bmod 8\,,$$

hence $p=c^2+2d^2=2s^2-t^2\equiv 1 \bmod 16$, and therefore $t\equiv\pm1 \bmod 8$.

Since $4\,|\,h_{8p}^+$, the classes P and Q are squares and we determine appropriate square roots. We observe that $(c,2d)=(t,2s)=1$, and we consider the classes

$$P_1=[\![c,-4d,-2c]\!]\in\mathfrak{F}_{8p}\quad\text{and}\quad Q_1=[\![t,-4s,2t]\!]\in\mathfrak{F}_{8p}\,.$$

Since $P_1^2=[\![c^2,-4d,-2]\!]$ represents -2 and $Q_1^2=[\![t^2,-4s,2]\!]$ represents 2, it follows by Theorem 6.4.13 that $P_1^2=P$ and $Q_1^2=Q$. For $n\in\mathbb{N}$, we obtain $2^{n+2}\,|\,h_{8p}^+$ if and only if both P_1 and Q_1 are 2^n-th powers. In particular, $8\,|\,h_{8p}^+$ if and only if P_1 and Q_1 are squares, which is equivalent to

$$\sigma(P_1)=\Big(\frac{c}{p}\Big)=1\quad\text{and}\quad \sigma(Q_1)=\Big(\frac{t}{p}\Big)=1\,.$$

This is just condition (a) of our criterion.

3. We continue to use the notations introduced hitherto and suppose that $8\,|\,h_{2p}^+$. Then $P_1,\ Q_1\in\mathfrak{F}_{8p}^2$, and there exist $c,\ d,\ s,\ t\in\mathbb{N}$ such that

$$t\equiv\pm1 \bmod 8\,,\quad \Big(\frac{c}{p}\Big)=1\quad\text{and}\quad p=c^2+2d^2=2s^2-t^2\,.$$

We assert that we can even achieve $t\equiv 1 \bmod 8$. Indeed, if $t\equiv -1 \bmod 8$, then $3t+4s\in\mathbb{N}$, $3t+4s\equiv 1 \bmod 8$, and since $p=2(2t+3s)^2-(3t+4s)^2$, we may replace (s,t) by $(2t+3s,3t+4s)$.

We have already proved that $16\,|\,h_{8p}^+$ if and only if the classes P_1 and Q_1 are both 4-th powers, and therefore it suffices to show:

$$\textbf{A.}\ \ P_1\in\mathfrak{F}_{8p}^4\iff\Big[\frac{c}{p}\Big]_4=1;\qquad \textbf{B.}\ \ Q_1\in\mathfrak{F}_{8p}^4\iff(-1)^{(t-1)/8}\Big(\frac{s}{t}\Big)=1\,.$$

Proof of **A.** Suppose that $P_1=R^2$, where $R=[\![r,*,*]\!]$ for some $r\in\mathbb{N}$ such that $(r,2pc)=1$. Then $P_1\in\mathfrak{F}_{8p}^4$ if and only if R is a square, that is, if and only if

$$\sigma(R)=\Big(\frac{r}{p}\Big)=1\,,\quad\text{and thus we must prove that}\quad \Big(\frac{r}{p}\Big)=\Big[\frac{c}{p}\Big]_4\,.$$

Since $R^2=P_1$ properly represents r^2, there exist $u,\ v\in\mathbb{Z}$ such that

$$(u,v)=1\quad\text{and}\quad r^2=cu^2-4duv-2cv^2\,.$$

As we may replace (u,v) by $(-u,-v)$, we may assume that $k=du+cv>0$. Then it follows that $cr^2=pu^2-2k^2$, $c\equiv 1 \bmod 8$ implies $2\,|\,k$, and $c\equiv -1 \bmod 8$ implies $2\nmid k$. Since $(k,2pc)=1$, we obtain

$$\Big[\frac{cr^2}{p}\Big]_4=\Big[\frac{c}{p}\Big]_4\Big(\frac{r}{p}\Big)=\Big[\frac{-2}{p}\Big]_4\Big(\frac{k}{p}\Big)=\Big[\frac{-1}{p}\Big]_4\Big[\frac{2}{p}\Big]_4\Big(\frac{k}{p}\Big)=\Big(\frac{k}{p}\Big)\,,$$

and therefore we must prove that

$$\Big(\frac{k}{p}\Big)=1\,.$$

CASE 1: $c \equiv 1 \bmod 8$. Since $k \equiv d \equiv 0 \bmod 2$, it follows that $v \equiv 0 \bmod 2$. We set $k = 2^\tau k_1$ and $v = 2^\omega v_1$, where $k_1,\ \tau,\ \omega \in \mathbb{N}$, $v_1 \in \mathbb{Z}$ and $2 \nmid k_1 v_1$. Finally, we observe the congruences

$$pu^2 \equiv cr^2 \bmod k_1\,, \quad k \equiv du \bmod c\,, \quad -4duv \equiv r^2 \bmod c\,, \quad cu^2 \equiv r^2 \bmod |v_1|$$

and that $(k,p) = (k,c) = (du,c) = (v,c) = 1$. Then we obtain

$$\Big(\frac{k}{p}\Big) = \Big(\frac{k_1}{p}\Big) = \Big(\frac{p}{k_1}\Big) = \Big(\frac{c}{k_1}\Big) = \Big(\frac{k_1}{c}\Big) = \Big(\frac{k}{c}\Big) = \Big(\frac{du}{c}\Big) = \Big(\frac{-v}{c}\Big)$$
$$= \Big(\frac{v_1}{c}\Big) = \Big(\frac{c}{|v_1|}\Big) = 1\,.$$

CASE 2: $c \equiv -1 \bmod 8$. Since $2 \nmid k$ and $4 \mid d$, it follows that $2 \nmid v$ and therefore $kv = duv + cv^2 \equiv -1 \bmod 4$. As in CASE 1, we obtain

$$\Big(\frac{k}{p}\Big) = \Big(\frac{p}{k}\Big) = \Big(\frac{c}{k}\Big) = (-1)^{(k-1)/2}\Big(\frac{k}{c}\Big) = (-1)^{(k-1)/2}\Big(\frac{-v}{c}\Big) = -(-1)^{(k-1)/2}\Big(\frac{v}{c}\Big)$$
$$= -(-1)^{(k-1)/2+(v-1)/2}\Big(\frac{c}{v}\Big) = -(-1)^{(kv-1)/2} = 1\,. \qquad \Box[\mathbf{A}.]$$

Proof of **B.** Suppose that $Q_1 = R^2$, where $R = [\![r,*,*]\!]$ for some $r \in \mathbb{N}$ such that $(r, 2pc) = 1$. It follows that $Q_1 \in \mathfrak{F}_{8p}^4$ if and only if R is a square, that is, if and only if

$$\sigma(R) = \Big(\frac{r}{p}\Big) = 1\,, \quad \text{and thus we must prove that} \quad \Big(\frac{r}{p}\Big) = (-1)^{(t-1)/8}\Big(\frac{s}{t}\Big)\,.$$

By Theorem 6.5.12 we obtain

$$\Big(\frac{r}{p}\Big) = \Big(\frac{2}{r}\Big) = (-1)^{(r^2-1)/8}\,.$$

Since R^2 properly represents r^2, there exist $u,\ v \in \mathbb{Z}$ such that

$$(u,v) = 1 \quad \text{and} \quad r^2 = tu^2 - 4suv - 2tv^2\,.$$

As we may replace (u,v) by $(-u,-v)$, we may assume that $k = su - tv > 0$. Then it follows that

$$tr^2 = 2k^2 - pu^2 \equiv 1 \bmod 8\,,$$

hence $2 \nmid ku$ and $tr^2 \equiv 2 - u^2 \equiv u^2 \bmod 16$. From this, we get

$$(-1)^{(r^2-1)/8+(t-1)/8} = (-1)^{(tr^2-1)/8} = (-1)^{(u^2-1)/8} = \Big(\frac{2}{|u|}\Big)\,.$$

Now we observe the congruences

$$2k^2 \equiv tr^2 \bmod |u|\,, \quad -4suv \equiv r^2 \bmod t \quad \text{and} \quad r^2 \equiv tu^2 \bmod |v|\,.$$

We obtain

$$\Big(\frac{2}{|u|}\Big) = \Big(\frac{t}{|u|}\Big) = \Big(\frac{|u|}{t}\Big) = \Big(\frac{u}{t}\Big) = \Big(\frac{sv}{t}\Big) = \Big(\frac{s}{t}\Big)\Big(\frac{t}{|v|}\Big) = \Big(\frac{s}{t}\Big)\,,$$

and thus finally

$$(-1)^{(r^2-1)/8} = (-1)^{(t-1)/8}\Big(\frac{s}{t}\Big)\,. \qquad \Box$$

This page intentionally left blank

APPENDIX A

Review of elementary algebra and number theory

This appendix contains an overview of the preliminaries in elementary algebra and number theory as far as they are used in this volume. Most of the material presented here should be familiar to a reader with a solid undergraduate training in algebra, and it will be sufficient to skim through the section headings. In many places of the main text, there are references to the required results from this appendix.

Besides standard material, the reader may find here a few rather special and generally less familiar algebraic and number-theoretical results (which however are presented with full proofs and referred to in the main text). In particular, I want to point out the following topics:

- Theorem A.3.7 on certain linear Diophantine equations,
- Sections A.4, A.5 and A.7 on finitely generated and finite abelian groups,
- Section A.6 on the structure of the prime residue class groups, and
- the elementary theory of algebraic integers as it is presented in Section A.9.

A.1. Fundamentals of group theory

By a *semigroup* S we mean a non-empty set together with an associative law of composition. If the composition is written additively [multiplicatively], we call S an *additive* [*multiplicative*] *semigroup.* A *monoid* is a semigroup possessing a neutral element (called its *unit element* and is usually denoted by 1 or e in the multiplicative case, and called its *zero element* and usually denoted by 0 in the additive case). An element u of a (multiplicative) monoid S with unit element e is called *invertible* if $uv = e$ for some (uniquely determined) element $v \in S$, and we call $v = u^{-1}$ the *inverse* of u. A *group* is a semigroup in which every element is invertible. The invertible elements of a monoid S form a group, denoted by $S^\times$ and called the *unit group* of S. Submonoids are assumed to contain the unit element, and monoid homomorphisms are assumed to respect the unit element. Commutative semigroups are called *abelian.*

We assume that the reader is familiar with the notions of subgroups and (group) homomorphisms and recall some further basis facts. Unless specified otherwise, we assume that all groups are multiplicative. Note that a homomorphism is called

- a *monomorphism* if it is injective;
- an *epimorphism* if it is surjective;
- an *isomorphism* if it is bijective.

We write $f\colon G \xrightarrow{\sim} G'$ if f is an isomorphism, and if $H \subset G$, then we denote by $H \hookrightarrow G$ the injection.

Subgroups, normal subgroups and factor groups. Let G be a (multiplicative) group with unit element e and H a subgroup of G. For $a \in G$, we call $aH = \{ax \mid x \in H\}$ the (*left*) *coset* of H determined by a and by G/H the set of all left cosets of H in G. Distinct cosets are disjoint, and therefore

$$G = \biguplus_{L \in G/H} L\,.$$

We call $(G\!:\!H) = |G/H|$ the *index* of H in G. Then $|G| = (G\!:\!H)\,|H|$ (Theorem of Lagrange). More generally, if $K \subset H \subset G$, then $(G\!:\!K) = (G\!:\!H)(H\!:\!K)$.

A subgroup H of G is called *normal* if $aH = Ha$ for all $a \in G$ [equivalently, $xax^{-1} \in H$ holds for all $x \in G$ and $a \in H$]. If $(G:H) = 2$, then H is a normal subgroup of G, and if G is abelian, then every subgroup of G is normal.

Assume now that H is a normal subgroup of G. Then G/H is a group with the induced composition, defined by $(aH)(bH) = abH$ for all $a,\, b \in G$. The residue class map $\pi\colon G \to G/H$, defined by $\pi(a) = aH$ for all $a \in G$, is an epimorphism. The group G/H is called the *factor group* of G by H. In particular, G itself is a normal subgroup of G, and G/G is the trivial group. The trivial subgroup $\{e\}$ of G is a normal subgroup, and the residue class homomorphism $G \to G/\{e\}$ is an isomorphism by means of which we identify these two groups: $G/\{e\} = G$. The assignment $U \mapsto U/H$ defines a bijective map from the set of all subgroups U of G which contain H onto the set of all subgroups of G/H, and the inverse map is given by $W \mapsto \pi^{-1}(W)$ for all subgroups W of G/H.

If $\varphi\colon G \to G_1$ is a homomorphism of (multiplicative) groups and e_1 is the unit element of G_1, then we denote by $\operatorname{Ker}(\varphi) = \varphi^{-1}(e_1) = \{x \in G \mid \varphi(x) = e_1\} \subset G$ its *kernel* and by $\operatorname{Im}(\varphi) = \varphi(G) \subset G_1$ its *image*. $\operatorname{Ker}(\varphi)$ is a normal subgroup of G, $\operatorname{Im}(\varphi)$ is a subgroup of G_1, and if φ is a monomorphism, then the induced map $\varphi\colon G \to \operatorname{Im}(\varphi)$ is a isomorphism.

Theorem A.1.1 (Main theorem on homomorphisms)**.** *Let $\varphi\colon G \to G_1$ be a group homomorphism.*

1. *Let H be a normal subgroup of G such that $H \subset \operatorname{Ker}(\varphi)$. Then there exists a unique homomorphism $\varphi_1\colon G/H \to G_1$ such that $\varphi_1(aH) = \varphi(a)$ for all $a \in G$. It satisfies $\operatorname{Ker}(\varphi_1) = \operatorname{Ker}(\varphi)/H$, and $\operatorname{Im}(\varphi_1) = \operatorname{Im}(\varphi)$. In particular, φ induces a monomorphism $\varphi_1\colon G/\operatorname{Ker}(\varphi) \to G_1$ and an isomorphism $\varphi_1\colon G/\operatorname{Ker}(\varphi) \xrightarrow{\sim} \operatorname{Im}(\varphi)$.*
2. *Let H_1 be a normal subgroup of G_1. Then $\varphi^{-1}(H_1)$ is a normal subgroup of G, and φ induces a monomorphism $\varphi_1\colon G/\varphi^{-1}(H_1) \to G_1/H_1$, given by $\varphi_1(a\varphi^{-1}(H_1)) = \varphi(a)H_1$. If φ is an epimorphism, then φ_1 is an isomorphism.*

Proof. 1. If $a,\, b \in G$, then $aH = bH$ implies $\varphi(a) = \varphi(b)$, since $H \subset \operatorname{Ker}(\varphi)$, and therefore there is a map $\varphi_1\colon G/H \to G_1$ such that $\varphi_1(aH) = \varphi(a)$ for all $a,\, b \in H$. Obviously, φ_1 is a group homomorphism which is uniquely determined by

φ, and $\operatorname{Im}(\varphi_1) = \operatorname{Im}(\varphi)$. If $a \in G$, then $aH \in \operatorname{Ker}(\varphi_1)$ if and only if $a \in \operatorname{Ker}(\varphi)$, and therefore $\operatorname{Ker}(\varphi_1) = \operatorname{Ker}(\varphi)/H$.

2. We consider the homomorphism $\varphi_0\colon G \to G_1/H_1$, defined by $\varphi_0(a) = \varphi(a)H_1$ for all $a \in G$. The $\operatorname{Ker}(\varphi_0) = \varphi^{-1}(H_1)$, hence $\varphi^{-1}(H_1)$ is a normal subgroup of G, and the assertion follows by 1. $\square$

Theorem A.1.2 (Isomorphism theorems)**.** *Let G be a (multiplicative) group.*

1. *Let H be a subgroup and N a normal subgroup of G. Then*
$$HN = \{ax \mid a \in H,\ x \in N\}$$
is a subgroup of G, N is a normal subgroup of HN, $H \cap N$ is a normal subgroup of H, and there is an isomorphism
$$\Phi\colon H/H\cap N \overset{\sim}{\to} HN/N\,, \quad \textit{given by} \quad \Phi(a(H\cap N)) = aN \ \ \textit{for all } a \in H.$$
2. *Let $H \subset N \subset G$ be normal subgroups. Then N/H is a normal subgroup of G/H, and there is an isomorphism*
$$\Psi\colon (G/H)/(N/H) \overset{\sim}{\to} G/N\,, \quad \textit{given by} \quad \Psi((aH)(N/H)) = aN$$
for all $a \in G$.

Proof. 1. We must show that u, $u_1 \in HN$ implies $uu_1^{-1} \in HN$. Thus suppose that $u = ax$ and $u_1 = a_1x_1$, where a, $a_1 \in H$ and x, $x_1 \in \mathbb{N}$. Then it follows that $uu_1^{-1} = axx_1^{-1}a_1^{-1} = aa_1^{-1}(a_1xx_1^{-1}a_1^{-1}) \in HN$, and we are done. Obviously, N is a normal subgroup of HN, and we define $\phi\colon H \to HN/N$ by $\phi(a) = aN$ for all $a \in H$. Then ϕ is a homomorphism, and if $a \in H$ and $x \in N$, then $axN = aN$. Hence ϕ is an epimorphism. Now $\operatorname{Ker}(\varphi) = N \cap H$ is a normal subgroup of H, and ϕ induces an isomorphism Φ as asserted by Theorem A.1.1.1.

2. We define $\psi\colon G/H \to G/N$ by $\psi(aH) = aN$. Then ψ is an epimorphism with kernel N/H, and the assertion follows by Theorem A.1.1.1. $\square$

Next we recall the notion of an exact sequence. Let $n \ge 2$ be an integer. For $i \in [1, n-1]$, let $\varphi_i\colon G_i \to G_{i+1}$ be a homomorphism of (multiplicative) groups. Then
$$\mathbf{1} \to G_1 \overset{\varphi_1}{\to} G_2 \overset{\varphi_2}{\to} G_3 \to \ldots \overset{\varphi_{n-1}}{\to} G_n \to \mathbf{1}$$
is called an *exact sequence* if φ_1 is a monomorphism, φ_{n-1} is an epimorphism, and $\operatorname{Ker}(\varphi_{i+1}) = \operatorname{Im}(\varphi_i)$ for all $i \in [1, n-1]$. If $n = 2$, this merely says that φ_1 is an isomorphism. If $n = 3$, then $\varphi_1(G_1)$ is a normal subgroup of G_2, and φ_2 induces an isomorphism $G_2/\varphi_1(G_1) \overset{\sim}{\to} G_3$. The following theorem shows how exact sequences can be used to calculate cardinalities.

Theorem A.1.3. *Let $n \ge 2$ be an integer and*
$$\mathbf{1} \to G_1 \overset{\varphi_1}{\to} G_2 \overset{\varphi_2}{\to} G_3 \to \ldots \overset{\varphi_{n-1}}{\to} G_n \to \mathbf{1}$$
an exact sequence of finite groups. Then
$$\prod_{j=1}^{n} |G_j|^{(-1)^j} = 1\,.$$

Proof. By induction on n.

$n = 2$: In this case, φ_1 is an isomorphism, and $|G_1| = |G_2|$.

$n \ge 3$, $n-1 \to n$: If $K = \operatorname{Ker}(\varphi_{n-1}) = \varphi_{n-2}(G_{n-2})$, then φ_{n-1} induces an isomorphism $G_{n-1}/K \overset{\sim}{\to} G_n$, and there is an exact sequence

$$\mathbf{1} \to G_1 \overset{\varphi_1}{\to} G_2 \to \ldots \to G_{n-2} \overset{\varphi_{n-2}}{\to} K \to \mathbf{1}\,.$$

Hence $|G_{n-1}| = |G_n|\,|K|$, and by the induction hypothesis we obtain

$$1 = \prod_{j=1}^{n-2} |G_j|^{(-1)^j} |K|^{(-1)^{n-1}} = \prod_{j=1}^{n-2} |G_j|^{(-1)^j} \left(\frac{|G_{n-1}|}{|G_n|} \right)^{(-1)^{n-1}} = \prod_{j=1}^{n} |G_j|^{(-1)^j}\,. \quad \square$$

Direct Products. If $n \in \mathbb{N}$ and $G_1, \ldots, G_n$ are (abelian) groups, then their cartesian product $G = G_1 \times \ldots \times G_n$ is an (abelian) group under component-wise composition. If K_i is a normal subgroup of G_i for all $i \in [1, n]$, then $K = K_1 \times \ldots \times K_n$ is a normal subgroup of G, and there is a (group) isomorphism

$$G/K \overset{\sim}{\to} G_1/K_1 \times \ldots \times G_n/K_n\,, \quad \text{given by} \quad (g_1, \ldots, g_n)K \mapsto (g_1K_1, \ldots, g_nK_n)\,.$$

By means of this isomorphism we identify these two groups.

If G is an abelian group, $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in G$, then we denote by

- $[a_1, \ldots, a_n] = \mathbb{Z}a_1 + \ldots + \mathbb{Z}a_n = \{k_1a_1 + \ldots + k_na_n \mid k_1, \ldots, k_n \in \mathbb{Z}\}$ the subgroup of G generated by $a_1, \ldots, a_n$ if G is an additive group (although we use brackets also to denote simple continued fractions and binary quadratic forms, there will be no danger of confusion);
- $\langle a_1, \ldots, a_n \rangle = \{a_1^{k_1} \cdot \ldots \cdot a_n^{k_n} \mid k_1, \ldots, k_n \in \mathbb{Z}\}$ the subgroup of G generated by $a_1, \ldots, a_n$ if G is an multiplicative group.

In both cases we call $\{a_1, \ldots, a_n\}$ a system of *generators* of G. If $f, g \colon G \to G_1$ are group homomorphisms, then $f = g$ if and only if $f(a_i) = g(a_i)$ for all $i \in [1, n]$.

A.2. Fundamentals of ring theory

By a ring R we always mean an associative and commutative ring with a unit element $1 \in R$. Note that a ring is both an additive group and multiplicative monoid. A subset T of a ring R is called a *subring* if it is both an additive subgroup and a multiplicative submonoid. Explicitly, T is a subring of R if and only if $1 \in T$ and $\{a - b, ab\} \subset T$ for all $a, b \in T$.

For a ring R, we denote by $R^\bullet = R \setminus \{0\}$ the set of its non-zero elements and by $R^\times$ the unit group of its multiplicative monoid (called the *unit group* of R). If $R = \{0\}$ [equivalently, if $1 = 0$], then we call R a *zero ring.* If R is a zero ring, then $R^\bullet = \emptyset$ and $R^\times = R$.

An element z of a ring R is called a *zero divisor* if $zy = 0$ for some $y \in R^\bullet$. An *integral domain* is a ring in which 0 is the only zero divisor, and a *field* is a ring R for which $R^\times = R^\bullet$. If R is an integral domain, then $1 \ne 0$, hence $|R| \ge 2$, and R possesses (up to isomorphisms) a unique quotient field denoted by $\mathsf{q}(R)$.

Recall that a field K is called a *quotient field* of R if R is a subring of K and $K = \{a^{-1}b \mid b \in R\,,\ a \in R^\bullet\}$.

A ring $R \neq \{0\}$ is an integral domain [a field] if and only if for every $a \in R^\bullet$ the map $\mu_a \colon R \to R$, defined by $\mu_a(x) = ax$, is injective [surjective]. Consequently, every finite integral domain is a field.

A map $f \colon R \to S$ of rings is a ring homomorphism if and only if it is both a homomorphism of multiplicative monoids and of additive groups. Explicitly, f is a ring homomorphism if and only if

$$f(1) = 1\,, \quad f(ab) = f(a)f(b) \ \text{ and } \ f(a+b) = f(a) + f(b) \ \text{ for all } a,\, b \in R.$$

If $f \colon R \to S$ is a ring homomorphism, then $f \,|\, R^\times \colon R^\times \to S^\times$ is a group homomorphism, and if f is an isomorphism, then $f \,|\, R^\times$ is also an isomorphism.

A subset $\mathfrak{a}$ of a ring R is called an *ideal* if it is an additive subgroup of R, and $R\mathfrak{a} = \{ra \mid r \in R,\ a \in \mathfrak{a}\} \subset \mathfrak{a}$. For an ideal $\mathfrak{a}$ of R, the (additive) factor group $R/\mathfrak{a}$ is a ring with addition and multiplication defined by

$$(x+\mathfrak{a}) + (y+\mathfrak{a}) = (x+y) + \mathfrak{a} \ \text{ and } \ (x+\mathfrak{a})(y+\mathfrak{a}) = xy + \mathfrak{a} \quad \text{for all } \ x,\, y \in R\,.$$

The residue class map $\pi \colon R \to R/\mathfrak{a}$, defined by $\pi(a) = a + \mathfrak{a}$ for all $a \in R$, is a ring epimorphism, and the assignment $\mathfrak{b} \mapsto \mathfrak{b}/\mathfrak{a}$ defines a bijective map from the set of all ideals $\mathfrak{b}$ of R containing $\mathfrak{a}$ onto the set of all ideals of $R/\mathfrak{a}$. The inverse map is given by $\mathfrak{q} \mapsto \pi^{-1}(\mathfrak{q})$ for all ideals $\mathfrak{q}$ of $R/\mathfrak{a}$. If $\mathfrak{a} \subset \mathfrak{b} \subset R$ are ideals, then the isomorphism of additive groups $(R/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a}) \overset{\sim}{\to} R/\mathfrak{b}$ given by Theorem A.1.2 is a ring isomorphism.

If $f \colon R \to S$ is a ring homomorphism, then its kernel $\mathfrak{a} = f^{-1}(0)$ is an ideal of R, f induces a ring monomorphism $f_1 \colon R/f^{-1}(0) \to S$ satisfying $f_1(x+\mathfrak{a}) = f(x)$ for all $x \in R$, and $\mathrm{Im}(f_1) = \mathrm{Im}(f)$ (see Theorem A.1.1).

$\{0\}$ and R are ideals of R, and if $\mathfrak{a}$ is any ideal of R, then $\mathfrak{a} = R$ if and only if $\mathfrak{a} \cap R^\times \neq \emptyset$. Obviously, R/R is a zero ring, and the residue class map $R \to R/\{0\}$ is an isomorphism. We identify: $R/R = \{0\}$ and $R/\{0\} = R$.

If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of a ring R, then their sum $\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a},\ b \in \mathfrak{b}\}$, their product $\mathfrak{a}\mathfrak{b} = \{a_1b_1 + \ldots + a_nb_n \mid n \in \mathbb{N},\ a_1, \ldots, a_n \in \mathfrak{a},\ b_1, \ldots, b_n \in \mathfrak{b}\}$ and their intersection $\mathfrak{a} \cap \mathfrak{b}$ are ideals of R, and $\mathfrak{a}\mathfrak{b} \subset \mathfrak{a} \cap \mathfrak{b}$. Addition and multiplication of ideals are associative and commutative composition laws satisfying the distributive law $(\mathfrak{a} + \mathfrak{b})\mathfrak{c} = \mathfrak{a}\mathfrak{c} + \mathfrak{b}\mathfrak{c}$ for all ideals $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ of R. If $n \in \mathbb{N}$ and $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ are ideals of R, then $\mathfrak{a}_1 + \ldots + \mathfrak{a}_n$ is the smallest ideal of R containing $\mathfrak{a}_1 \cup \ldots \cup \mathfrak{a}_n$. In particular, if $a_1, \ldots, a_n \in R$, then $a_1R + \ldots + a_nR$ is the smallest ideal of R containing $\{a_1, \ldots, a_n\}$. We call $a_1R + \ldots + a_nR$ the *ideal generated by* $a_1, \ldots, a_n$.

An ideal $\mathfrak{a}$ of a ring R is called a *principal ideal* if $\mathfrak{a} = aR$ for some $a \in R$. A *principal ideal domain* is an integral domain in which every ideal is a principal ideal.

An ideal $\mathfrak{a}$ of a ring R is called

- a *prime ideal* if $R/\mathfrak{a}$ is an integral domain [equivalently, $\mathfrak{a} \neq R$, and if $a,\, b \in R \setminus \mathfrak{a}$, then $ab \in R \setminus \mathfrak{a}$] ;
- a *maximal ideal* if $\mathfrak{a} \neq R$, and there is no ideal $\mathfrak{b}$ such that $\mathfrak{a} \subsetneq \mathfrak{b} \subsetneq R$ [equivalently, $R/\mathfrak{a}$ is a field].

Every maximal ideal is a prime ideal. If $\mathfrak{p}$ is a prime ideal of R, $n \in \mathbb{N}$ and $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ are any ideals of R, then $\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n \subset \mathfrak{p}$ implies $\mathfrak{a}_i \subset \mathfrak{p}$ for some $i \in [1, n]$.

We assume that the reader is familiar with the basic notions of polynomials. Polynomial rings over a ring R are denoted by $R[X]$, $R[X, Y]$, $R[X_1, \ldots, X_n]$ etc. without any further specification.

Suppose that $f \in R[X]$. Then f has a unique representation

$$f = \sum_{n \geq 0} a_n X^n \quad \text{where} \quad a_n \in R \quad \text{and} \quad a_n = 0 \quad \text{for almost all} \quad n \geq 0\,,$$

and we call $\deg(f) = \sup\{n \geq 0 \mid a_n \neq 0\} \in \mathbb{N}_{\geq 0} \cup \{-\infty\}$ its *degree* (in particular, $\deg(0) = -\infty$). For $\alpha \in R$, we set

$$f(\alpha) = \sum_{n \geq 0} a_n \alpha^n \in R\,,$$

and α is called a *zero* of f if $f(\alpha) = 0$ [equivalently, $f = (X - \alpha)g$ for some polynomial $g \in R[X]$].

We recall without proof the main properties of polynomials over integral domains.

Polynomials over integral domains. Let R be an integral domain. Then

- $\deg(fg) = \deg(f) + \deg(g)$ for all polynomials f, $g \in R[X]$.
- $R[X]$ is an integral domain, and $R[X]^\times = R^\times$.
- If $f \in R[X]$ and $\deg(f) = n \geq 0$, then f has at most n zeros in $R[X]$.

For a ring R and m, $n \in \mathbb{N}$, we denote by $\mathsf{M}_{m,n}(R)$ the set of all (m, n)-matrices $A = (a_{j,i})_{j \in [1,m],\, i \in [1,n]}$ with entries $a_{j,i} \in R$, and for $A \in \mathsf{M}_{m,n}(R)$, we denote by $A^{\mathsf{t}} \in \mathsf{M}_{n,m}(R)$ its transpose. Then $\mathsf{M}_n(R) = \mathsf{M}_{n,n}(R)$ is a ring with unit group

$$\mathsf{GL}_n(R) = \mathsf{M}_n(R)^\times = \{A \in \mathsf{M}_n(R) \mid \det(A) \in R^\times\}\,,$$

and we set $\mathsf{SL}_n(R) = \{A \in \mathsf{M}_n(R) \mid \det(A) = 1\}$. As $\det\colon \mathsf{GL}_n(R) \to R^\times$ is a group homomorphism with kernel $\mathsf{SL}_n(R)$, it follows that $\mathsf{SL}_n(R)$ is a normal subgroup of $\mathsf{GL}_n(R)$, and $(\mathsf{GL}_n(R) : \mathsf{SL}_n(R)) = |R^\times|$. For $(d_1, \ldots, d_n) \in R^n$, we denote by $\operatorname{diag}(d_1, \ldots, d_n) \in \mathsf{M}_n(R)$ the diagonal matrix with entries $d_1, \ldots, d_n$. In particular, $I_n = \operatorname{diag}(1, \ldots, 1)$ denotes the unit matrix.

Direct Products. If $R_1, \ldots, R_n$ are rings, then $R = R_1 \times \ldots \times R_n$ is a ring under component-wise addition and multiplication, and $R^\times = R_1^\times \times \ldots \times R_n^\times$. If $\mathfrak{a}_i$ is an ideal of R_i for all $i \in [1, n]$, then $\mathfrak{a} = \mathfrak{a}_1 \times \ldots \times \mathfrak{a}_n$ is an ideal of R, and there is a natural isomorphism $R/\mathfrak{a} \overset{\sim}{\to} R_1/\mathfrak{a}_1 \times \ldots \times R_n/\mathfrak{a}_n$ by means of which we identify these two rings.

Congruences. Let R be a ring and $\mathfrak{a}$ an ideal of R. Two elements a, $b \in R$ are called *congruent* modulo $\mathfrak{a}$, and we write $a \equiv b \bmod \mathfrak{a}$ if $a - b \in \mathfrak{a}$ [equivalently, $a + \mathfrak{a} = b + \mathfrak{a} \in R/\mathfrak{a}$]. If $\mathfrak{a} = dR$ for some $d \in R$, then we write $a \equiv b \bmod d$ (in R) instead of $a \equiv b \bmod dR$, and we say that a and b are congruent modulo d (in R).

If a, b, a', $b' \in R$, $a \equiv b \bmod \mathfrak{a}$ and $a' \equiv b' \bmod \mathfrak{a}$, then $a + a' \equiv b + b' \bmod \mathfrak{a}$ and $aa' \equiv bb' \bmod \mathfrak{a}$.

The most important result on congruences is the Chinese remainder theorem. Although well known, we prove it here.

Theorem A.2.1 (Chinese remainder theorem)**.** *Let R be a ring, $r \in \mathbb{N}$, and let $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ be ideals of R such that $\mathfrak{a}_i + \mathfrak{a}_j = R$ for all $i,\, j \in [1, r]$ with $i \neq j$. Then $\mathfrak{a} = \mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_r = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_r$, the map $\Phi_0 \colon R \to R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_r$, defined by $\Phi_0(x) = (x + \mathfrak{a}_1, \ldots, x + \mathfrak{a}_r)$ for all $x \in R$, is a ring epimorphism, and* $\mathrm{Ker}(\Phi_0) = \mathfrak{a}$*. Φ_0 induces a ring isomorphism*

$\Phi \colon R/\mathfrak{a} \overset{\sim}{\to} R/\mathfrak{a}_1 \times \ldots \times R/\mathfrak{a}_r$ satisfying $\Phi(x + \mathfrak{a}) = (x + \mathfrak{a}_1, \ldots, x + \mathfrak{a}_n)$ for all $x \in R$

and $\Phi \,|\, (R/\mathfrak{a})^\times \colon (R/\mathfrak{a})^\times \overset{\sim}{\to} (R/\mathfrak{a}_1)^\times \times \ldots \times (R/\mathfrak{a}_r)^\times$ is a group isomorphism.

Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of a ring R such that $\mathfrak{a} + \mathfrak{b} = R$ are called *coprime*. More generally, if $n \in \mathbb{N}$ and $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ are ideals of R, then $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ are called

- *coprime* if $\mathfrak{a}_1 + \ldots + \mathfrak{a}_n = R$;
- *pairwise coprime* if $\mathfrak{a}_i + \mathfrak{a}_j = R$ for all $i,\, j \in [1, n]$ such that $i \neq j$.

Proof of Theorem A.2.1. By definition, Φ_0 is a ring homomorphism, and $\mathrm{Ker}(\Phi_0) = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_r$. We prove by induction on r that $\mathfrak{a} = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_r$, and that for any $(x_1, \ldots, x_r) \in R^r$ there exists some $x \in R$ such that $x \equiv x_i \mod \mathfrak{a}_i$ for all $i \in [1, r]$. Then Φ_0 is surjective, and the remaining assertions are obvious. For $r = 1$ there is nothing to do.

$r = 2$: Since $\mathfrak{a}_1 + \mathfrak{a}_2 = R$, there exist $a_1 \in \mathfrak{a}_1$ and $a_2 \in \mathfrak{a}_2$ such that $a_1 + a_2 = 1$. If $c \in \mathfrak{a}_1 \cap \mathfrak{a}_2$, then $c = ca_1 + ca_2 \in \mathfrak{a}_1\mathfrak{a}_2$. Hence $\mathfrak{a}_1 \cap \mathfrak{a}_2 \subset \mathfrak{a}_1\mathfrak{a}_2$, and the other inclusion is obvious.

If $(x_1, x_2) \in R^2$, then $x = a_1x_2 + a_2x_1 = x_1 + a_1(x_2 - x_1) = x_2 + a_2(x_1 - x_2) \in R$, $x \equiv x_1 \mod \mathfrak{a}_1$ and $x \equiv x_2 \mod \mathfrak{a}_2$.

$r \geq 3$, $r - 1 \to r$: For $i \in [2, r]$, let $a_i \in \mathfrak{a}_1$ and $b_i \in \mathfrak{a}_i$ be such that $a_i + b_i = 1$. Then

$$1 = \prod_{i=2}^{r} (a_i + b_i) = a + b_2 \cdot \ldots \cdot b_r \quad \text{for some} \;\; a \in \mathfrak{a}_1\,,$$

and therefore $\mathfrak{a}_1 + \mathfrak{a}_2 \cdot \ldots \cdot \mathfrak{a}_r = R$. By the induction hypothesis and the case $r = 2$ it follows that $\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_r = \mathfrak{a}_1 \cdot (\mathfrak{a}_2 \cdot \ldots \cdot \mathfrak{a}_r) = \mathfrak{a}_1 \cap (\mathfrak{a}_2 \cap \ldots \cap \mathfrak{a}_r) = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_r$.

If $(x_1, \ldots, x_r) \in R^r$, then the induction hypothesis implies that there exists some $y \in R$ such that $y \equiv x_i \mod \mathfrak{a}_i$ for all $i \in [2, r]$, and (by the case $r = 2$) there exists some $x \in R$ such that $x \equiv x_1 \mod \mathfrak{a}_1$ and $x \equiv y \mod \mathfrak{a}_2 \cdot \ldots \cdot \mathfrak{a}_r$. Hence it follows that $x \equiv y \equiv x_i \mod \mathfrak{a}_i$ for all $i \in [2, r]$. ☐

A.3. Elementary arithmetic in $\mathbb{Z}$

We recall some elementary and well-known facts (mostly without proofs).

Division with remainder. Suppose that $b \in \mathbb{Z}^\bullet$, $c \in \mathbb{Z}$, $a \in \mathbb{R}$ and either $J = [c, c + |b|)$ or $J = (c, c + |b|]$. Then there exists a unique pair $(q, r) \in \mathbb{Z} \times \mathbb{R}$ such that $a = bq + r$ and $r \in J$.

In particular, if $a \in \mathbb{Z}$ and $b \in \mathbb{N}$, then there exist uniquely determined integers $q \in \mathbb{Z}$ and $r \in [c, c + b - 1]$ such that $a = bq + r$.

Ideals and divisibility. $\mathbb{Z}$ is a principal ideal domain. If $\mathfrak{a}$ is a non-zero ideal of $\mathbb{Z}$ and $a \in \mathbb{N}$, then $a = \min(\mathfrak{a} \cap \mathbb{N})$ if and only if $\mathfrak{a} = a\mathbb{Z}$. For $a,\, b \in \mathbb{Z}$, we call a a *divisor* of b and b a *multiple* of a if $b = ac$ for some $c \in \mathbb{Z}$ [equivalently, $b \in a\mathbb{Z}$ or $b\mathbb{Z} \subset a\mathbb{Z}$]. In this case, we write $a \,|\, b$.

Greatest common divisor. If $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in \mathbb{Z}$, then there exists a unique integer $d \in \mathbb{N}_0$ such that the following conditions are fulfilled:

- $d \,|\, a_i$ for all $i \in [1, n]$;
- if $g \in \mathbb{Z}$ is such that $g \,|\, a_i$ for all $i \in [1, n]$, then $g \,|\, d$.

If these conditions are fulfilled, then d is called the *greatest common divisor* of $a_1, \ldots, a_n$. We write $d = \gcd(a_1, \ldots, a_n)$ or simply $d = (a_1, \ldots, a_n)$ if there is no danger of confusion.

If $d \in \mathbb{N}_0$, then $d = (a_1, \ldots, a_n)$ if and only if $d\mathbb{Z} = a_1\mathbb{Z} + \ldots + a_n\mathbb{Z}$ [equivalently, $d \,|\, a_i$ for all $i \in [1, n]$, and there exist $x_1, \ldots, x_n \in \mathbb{Z}$ such that $d = a_1x_1 + \ldots + a_nx_n$]. In particular, $(a_1, \ldots, a_n) = 1$ if and only if there exist $x_1, \ldots, x_n \in \mathbb{Z}$ such that $a_1x_1 + \ldots + a_nx_n = 1$, and in this case the numbers $a_1, \ldots, a_n$ are called *coprime.* Note that $a_1, \ldots, a_n$ are coprime if and only if the ideals $a_1\mathbb{Z}, \ldots, a_n\mathbb{Z}$ are coprime.

If $a,\, b \in \mathbb{N}$ and $d = (a, b)$, then there exist $x,\, y \in \mathbb{N}$ such that $d = ax - by$. If $g \in \mathbb{Q}$ and $ga_i \in \mathbb{Z}$ for all $i \in [1, n]$, then $(ga_1, \ldots, ga_n) = |g|\,(a_1, \ldots, a_n)$.

For all $a,\, b,\, c \in \mathbb{Z}$ the following assertions hold (for more general statemens, see Theorem A.8.2):

- If $a \,|\, bc$ and $(a, b) = 1$, then $a \,|\, c$.
- If $(a, b) = (a, c) = 1$, then $(a, bc) = 1$.

For $a,\, b \in \mathbb{N}$, the greatest common divisor (a, b) can be calculated by means of the Euclidean algorithm, which consists of a sequence of $k+1$ divisions with remainder (for some $k \in \mathbb{N}_0$) as follows:

$$\begin{aligned}
r_{-1} = a &= u_0 b + r_1\,, && \text{where} \quad u_0 \in \mathbb{Z}\,,\ r_1 \in [1, q-1]\,,\\
r_0 = b &= u_1 r_1 + r_2\,, && \text{where} \quad u_1 \in \mathbb{N}\,,\ r_2 \in [1, r_1 - 1]\,,\\
r_1 &= u_2 r_2 + r_3\,, && \text{where} \quad u_2 \in \mathbb{N}\,,\ r_3 \in [1, r_2 - 1]\,,\\
&\ \vdots\\
r_{k-2} &= u_{k-1} r_{k-1} + r_k\,, && \text{where} \quad u_{k-1} \in \mathbb{N}\,,\ r_k \in [1, r_{k-1}]\,,\\
r_{k-1} &= u_k r_k\,, && \text{where} \quad u_k \in \mathbb{N}\,,\ u_k \geq 2\,.
\end{aligned}$$

Then it follows that $r_k = (a, b)$.

Least common multiple. Let $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in \mathbb{Z}$. Then there is a unique integer $e \in \mathbb{N}_0$ such that the following conditions are fulfilled:

- $a_i \,|\, e$ for all $i \in [1, n]$;
- if $g \in \mathbb{Z}$ is such that $a_i \,|\, g$ for all $i \in [1, n]$, then $e \,|\, g$.

If these conditions are fulfilled, then e is called the *least common multiple* of $a_1, \ldots, a_n$, and we write $e = \operatorname{lcm}(a_1, \ldots, a_n)$. If $e \in \mathbb{N}_0$, then $e = \operatorname{lcm}(a_1, \ldots, a_n)$ if and only if $e\mathbb{Z} = a_1\mathbb{Z} \cap \ldots \cap a_n\mathbb{Z}$, and $|ab| = \gcd(a, b) \operatorname{lcm}(a, b)$ for all $a, b \in \mathbb{Z}$.

If $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in \mathbb{Z}$, then

$$(a_1, \ldots, a_n) = (|a_1|, \ldots, |a_n|)\,, \quad \operatorname{lcm}(a_1, \ldots, a_n) = \operatorname{lcm}(|a_1|, \ldots, |a_n|)\,,$$

and if $n \geq 2$, then

$$(a_1, \ldots, a_n) = ((a_1, \ldots, a_{n-1}), a_n)\,, \quad \operatorname{lcm}(a_1, \ldots, a_n) = \operatorname{lcm}(\operatorname{lcm}(a_1, \ldots, a_{n-1}), a_n)\,.$$

The following Theorem A.3.1 is used in Section 4.1.

Theorem A.3.1. *Suppose that a, r, $m_1, \ldots, m_r \in \mathbb{N}$ and $a \geq 2$. Then*

$$(a^{m_1} - 1, \ldots, a^{m_r} - 1) = a^{(m_1, \ldots, m_r)} - 1\,.$$

Proof. By induction on r. For $r = 1$ there is nothing to do.

$r = 2$: Let $d = (m_1, m_2)$ and $x_1, x_2 \in \mathbb{N}$ be such that $d = m_1x_1 - m_2x_2$. Then $a^d - 1$ divides $(a^{m_1} - 1, a^{m_2} - 1)$, and we must prove that every common divisor of $a^{m_1} - 1$ and $a^{m_2} - 1$ divides $a^d - 1$. Thus let $k \in \mathbb{N}$ be a common divisor of $a^{m_1} - 1$ and $a^{m_2} - 1$. Since $a^{m_i} - 1$ divides $a^{m_ix_i} - 1$ for $i \in \{1, 2\}$, it follows that k divides $a^{m_1x_1} - 1$ and $a^{m_2x_2} - 1$. Hence k divides

$$a^{m_1x_1} - a^{m_2x_2} = a^{m_2x_2}(a^{m_1x_1 - m_2x_2} - 1) = a^{m_2x_2}(a^d - 1)\,,$$

and since $(k, a) = 1$, it follows that k divides $a^d - 1$.

$r \geq 3$, $r - 1 \to r$: By the induction hypothesis and the case $r = 2$, we obtain

$$\begin{aligned}(a^{m_1} - 1, \ldots, a^{m_r} - 1) &= ((a^{m_1} - 1, \ldots, a^{m_{r-1}} - 1), a^{m_r} - 1) \\ &= (a^{(m_1, \ldots, m_{r-1})} - 1, a^{m_r} - 1) = a^{((m_1, \ldots, m_{r-1}), m_r)} - 1 \\ &= a^{(m_1, \ldots, m_r)} - 1\,. \end{aligned}$$

□

Reduced fractions. Every $r \in \mathbb{Q}$ has a unique representation

$$r = \frac{p}{q}\,, \quad \text{where} \quad p \in \mathbb{Z}\,,\ q \in \mathbb{N} \ \text{ and } \ (p, q) = 1\,.$$

We call p the *reduced numerator* and q the *reduced denominator* of r (for a more general statement see Theorem A.8.3.4). The following slightly more precise result is used in the proof of Theorem 1.1.2.

Theorem A.3.2. *If $n \in \mathbb{N}$, $r_1, \ldots, r_n \in \mathbb{Q}$ and $\varepsilon \in \{\pm 1\}$, then there exist uniquely determined integers a, $b_1, \ldots, b_n \in \mathbb{Z}$ such that*

$$\operatorname{sgn}(a) = \varepsilon\,, \quad (a, b_1, \ldots, b_n) = 1 \quad \textit{and} \quad r_i = \frac{b_i}{a} \quad \textit{for all} \quad i \in [1, n]\,.$$

Proof. *Existence*: Let $d \in \mathbb{N}$ be a common denominator of $r_1, \ldots, r_n$, and let $c_1, \ldots, c_n \in \mathbb{Z}$ be such that

$$r_i = \frac{c_i}{d} \quad \text{for all } i \in [1, n]\,.$$

If $g = (c_1, \ldots, c_n, d)$, then there exist integers $a,\ b_1, \ldots, b_n \in \mathbb{Z}$ are such that $\varepsilon d = ag$ and $\varepsilon c_i = b_i g$ for all $i \in [1, n]$. It follows that $(b_1, \ldots, b_n, a) = 1$, $\operatorname{sgn}(a) = \varepsilon$, and

$$r_i = \frac{c_i}{d} = \frac{\varepsilon b_i g}{\varepsilon a g} = \frac{b_i}{a} \quad \text{for all} \quad i \in [1, n]\,.$$

Uniqueness: Let $a,\ a',\ b_1, \ldots, b_n,\ b_1', \ldots, b_n' \in \mathbb{Z}$ be such that $\operatorname{sgn}(a) = \operatorname{sgn}(a')$,

$$r_i = \frac{b_i}{a} = \frac{b_i'}{a'} \ \text{ for all } \ i \in [1, n]\,, \quad \text{and} \quad (a, b_1, \ldots, b_n) = (a', b_1', \ldots, b_n') = 1\,.$$

Then it follows that $ab_i' = a'b_i$ for all $i \in [1, n]$, and

$$|a'| = (a'a,\ a'b_1, \ldots, a'b_n) = (aa',\ ab_1', \ldots, ab_n') = |a|\,.$$

Hence $a = a'$ and therefore $b_i = b_i'$ for all $i \in [1, n]$. □

Fundamental theorem of arithmetic. The set $\mathbb{P}$ of primes is infinite, and every $a \in \mathbb{N}$ has a unique factorization $a = p_1 \cdot \ldots \cdot p_n$, where $n \in \mathbb{N}_0$, $p_1, \ldots, p_n$ are primes, and $p_1 \le \ldots \le p_n$.

More generally, every $a \in \mathbb{Q}^\times$ has a unique representation as a (formally infinite) product

$$a = \varepsilon \prod_{p \in \mathbb{P}} p^{\mathsf{v}_p(a)},$$

where $\varepsilon \in \{\pm 1\}$, $\mathsf{v}_p(a) \in \mathbb{Z}$ and $\mathsf{v}_p(a) = 0$ for almost all primes p.

For every prime p, the exponent $\mathsf{v}_p(a)$ in the above representation of $a \in \mathbb{Q}^\times$ is called the *p-adic value* of a. We set $\mathsf{v}_p(0) = \infty$ and call $\mathsf{v}_p \colon \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ the *p-adic valuation.* If $a,\ b \in \mathbb{Q}$, then

$$\mathsf{v}_p(ab) = \mathsf{v}_p(a) + \mathsf{v}_p(b) \ \text{ and } \ \mathsf{v}_p(a+b) \ge \min\{\mathsf{v}_p(a), \mathsf{v}_p(b)\} \ \text{ for all primes } \ p\,.$$

By definition, $\mathbb{Z} = \{a \in \mathbb{Q} \mid \mathsf{v}_p(a) \ge 0 \text{ for all primes } p\}$, and if $a,\ b \in \mathbb{Z}$, then $a \,|\, b$ if and only if $\mathsf{v}_p(a) \le \mathsf{v}_p(b)$ for all primes p.

If p is a prime, then every $x \in \mathbb{Q}^\times$ has a unique representation

$$x = p^n \,\frac{b}{a}\,, \quad \text{where} \quad n = \mathsf{v}_p(x)\,,\ b \in \mathbb{Z}\,,\ a \in \mathbb{N}\,,\ p \nmid ab \ \text{ and } \ (a, b) = 1\,.$$

The greatest common divisor and the least common multiple can be calculated by means of the p-adic values as follows. If $n \in \mathbb{N}$, $a_1, \ldots, a_n \in \mathbb{Z}$ and $d,\ e \in \mathbb{N}_0$, then

$$d = (a_1, \ldots, a_n) \iff \mathsf{v}_p(d) = \min\{\mathsf{v}_p(a_1), \ldots, \mathsf{v}_p(a_n)\} \ \text{ for all primes } \ p\,,$$

and

$$e = \operatorname{lcm}(a_1, \ldots, a_n) \iff \mathsf{v}_p(d) = \max\{\mathsf{v}_p(a_1), \ldots, \mathsf{v}_p(a_n)\} \ \text{ for all primes } \ p\,.$$

Squares. A rational number r is called a *square* if $r = q^2$ for some $q \in \mathbb{Q}_{\ge 0}$. If $r \in \mathbb{Q}^\times$, then r is a square if and only if $r > 0$ and $2 \,|\, \mathsf{v}_p(r)$ for all primes p. If $r \in \mathbb{Z}$, then r is a square if and only if $r = q^2$ for some $q \in \mathbb{N}_0$.

An integer d is called *squarefree* if there is no integer $e \ge 2$ such that $e^2 \,|\, d$ [equivalently, $\mathsf{v}_p(d) \in \{0, 1\}$ for all primes p].

Theorem and Definition A.3.3 (Squarefree kernels)**.**

1. *If* $d_1,\, d_2 \in \mathbb{Z}$ *are squarefree and* $d_2 = d_1q^2$ *for some* $q \in \mathbb{Q}_{>0}$*, then* $q = 1$.
2. *For every* $d \in \mathbb{Q}^\times$ *there exists a unique squarefree integer* $d_0 \in \mathbb{Z}$ *such that* $d = d_0q^2$ *for some* $q \in \mathbb{Q}_{>0}$*. It is given by*

$$d_0 = \operatorname{sgn}(d) \prod_{\substack{p \in \mathbb{P} \\ 2 \nmid \mathsf{v}_p(d)}} p\,, \quad \text{and then} \quad q = \prod_{p \in \mathbb{P}} p^{\lfloor \mathsf{v}_p(d)/2 \rfloor}\,.$$

In particular, if $d \in \mathbb{Z}$*, then it follows that* $q \in \mathbb{N}$.

d_0 it is called the *squarefree kernel* of d.

Proof. 1. Let $d_1,\, d_2 \in \mathbb{Z}$ be squarefree and $q \in \mathbb{Q}_{>0}$ such that $d_2 = d_1q^2$. For every prime p we have $2\mathsf{v}_p(q) = \mathsf{v}_p(d_2) - \mathsf{v}_p(d_1)$, and since $\mathsf{v}_p(d_1),\, \mathsf{v}_p(d_2) \in \{0,1\}$, we obtain $\mathsf{v}_p(q) = 0$, and consequently $q = 1$.

2. If

$$d_0 = \operatorname{sgn}(d) \prod_{\substack{p \in \mathbb{P} \\ 2 \nmid \mathsf{v}_p(d)}} p\,, \quad \text{then} \quad d_0^{-1}d = \prod_{\substack{p \in \mathbb{P} \\ 2 \nmid \mathsf{v}_p(d)}} p^{\mathsf{v}_p(d)-1} \prod_{\substack{p \in \mathbb{P} \\ 2 \mid \mathsf{v}_p(d)}} p^{\mathsf{v}_p(d)} = \Bigl[\prod_{p \in \mathbb{P}} p^{\lfloor \mathsf{v}_p(d)/2 \rfloor}\Bigr]^2,$$

$d_0 \in \mathbb{Z}$ is squarefree, and $d_0^{-1}d = q^2$ for some $q \in \mathbb{Q}_{>0}$. This proves the existence of a squarefree kernel, and its uniqueness follows by 1. □

Congruences. For $a,\, b \in \mathbb{Z}$ and $m \in \mathbb{N}$, we write $a \equiv b \bmod m$ and call a and b *congruent modulo* m if $a \equiv b \bmod m\mathbb{Z}$ [equivalently, $a + m\mathbb{Z} = b + m\mathbb{Z}$ or $m \mid b - a$]. For every $b \in \mathbb{Z}$, we have $\mathbb{Z}/m\mathbb{Z} = \{j + m\mathbb{Z} \mid j \in [b+1, b+m]\}$.

If $a,\, b \in \mathbb{Z}$ and $m \in \mathbb{N}$, then

- $a \equiv b \bmod m$ implies $(a,m) = (b,m)$;
- there is some $x \in \mathbb{Z}$ such that $ax \equiv b \bmod m$ if and only if $(a,m) \mid b$, and then

$$ax \equiv b \mod m \quad \iff \quad x \equiv \frac{b}{(a,m)} \mod \frac{m}{(a,m)}\,.$$

If $r \in \mathbb{N}$, $m_1, \ldots, m_r \in \mathbb{N}$ and $m = \operatorname{lcm}(m_1, \ldots, m_r)$, then $a \equiv b \bmod m$ holds if and only if $a \equiv b \bmod m_i$ for all $i \in [1,r]$.

The following simple lemma is often used throughout this volume.

Lemma A.3.4. *Suppose that* $k,\, n \in \mathbb{N}$, $t_1, \ldots, t_n \in \mathbb{Z}$ *and* $t_i \equiv 1 \bmod k$ *for all* $i \in [1,n]$*. Then*

$$\sum_{i=1}^n \frac{t_i - 1}{k} \equiv \frac{t_1 \cdot \ldots \cdot t_n - 1}{k} \mod k\,.$$

Proof. For $i \in [1,n]$, we set $t_i = ks_i + 1$, where $s_i \in \mathbb{Z}$, and then we obtain

$$\prod_{i=1}^n t_i - 1 = \prod_{i=1}^n (ks_i + 1) - 1 \equiv \sum_{i=1}^n ks_i \equiv \sum_{i=1}^n (t_i - 1) \mod k^2\,.$$

Dividing by k implies the assertion. □

Because of its importance, we reformulate the Chinese remainder theorem A.2.1 for the integers and amend the assertions of the general case.

Theorem A.3.5 (Chinese remainder theorem for $\mathbb{Z}$)**.**

1. *Suppose that* $r, m_1, \ldots, m_r \in \mathbb{N}$, $m = m_1 \cdot \ldots \cdot m_r$ *and* $(m_i, m_j) = 1$ *for all* $i,\ j \in [1, r]$ *such that* $i \neq j$. *Then there is a ring isomorphism*
$$\Phi\colon \mathbb{Z}/m\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_r\mathbb{Z}$$
such that $\Phi(x + m\mathbb{Z}) = (x + m_1\mathbb{Z}, \ldots, x + m_r\mathbb{Z})$ *for all* $x \in \mathbb{Z}$, *and*
$$\Phi \,|\, (\mathbb{Z}/m\mathbb{Z})^\times \colon (\mathbb{Z}/m\mathbb{Z})^\times \xrightarrow{\sim} (\mathbb{Z}/m_1\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/m_r\mathbb{Z})^\times$$
is a group isomorphism.
2. *If* $m_1,\ m_2 \in \mathbb{N}$, $(m_1, m_2) = 1$ *and* $m = m_1 m_2$, *then there is a bijective map*
$$\Psi\colon \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \ \to\ \mathbb{Z}/m\mathbb{Z}$$
such that $\Psi(t_1 + m_1\mathbb{Z}, t_2 + m_2\mathbb{Z}) = t_1 m_2 + t_2 m_1 + m\mathbb{Z}$ *for all* $t_1,\ t_2 \in \mathbb{Z}$. *It satisfies* $\Psi((\mathbb{Z}/m_1\mathbb{Z})^\times \times (\mathbb{Z}/m_2\mathbb{Z})^\times) = (\mathbb{Z}/m\mathbb{Z})^\times$.

PROOF. 1. If $(m_i, m_j) = 1$, then $m_i\mathbb{Z} + m_j\mathbb{Z} = \mathbb{Z}$ for all $i,\ j \in [1, r]$ such that $i \neq j$, and the assertions follow by Theorem A.2.1.

2. For $(t_1, t_2) \in \mathbb{Z}^2$, the residue class $t_1m_2 + t_2m_1 + m\mathbb{Z} \in \mathbb{Z}/m\mathbb{Z}$ only depends on the residue classes $t_1 + m_1\mathbb{Z} \in \mathbb{Z}/m_1\mathbb{Z}$ and $t_2 + m_2\mathbb{Z} \in \mathbb{Z}/m_2\mathbb{Z}$. Hence there is a map $\Psi\colon \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ such that $\Psi(t_1 + m_1\mathbb{Z}, t_2 + m_2\mathbb{Z}) = t_1m_2 + t_2m_1 + m\mathbb{Z}$ for all $t_1,\ t_2 \in \mathbb{Z}$.

Since $|\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}| = |\mathbb{Z}/m\mathbb{Z}|$ and $|(\mathbb{Z}/m_1\mathbb{Z})^\times \times (\mathbb{Z}/m_2\mathbb{Z})^\times| = |(\mathbb{Z}/m\mathbb{Z})^\times|$, it suffices to prove: **1)** Ψ is injective; **2)** If $(t_1, t_2) \in \mathbb{Z}^2$ and $(t_1, m_1) = (t_2, m_2) = 1$, then $(t_1m_2 + t_2m_1, m) = 1$.

1) If $(t_1, t_2),\ (t_1', t_2') \in \mathbb{Z}^2$ and $t_1m_2 + t_2m_1 + m\mathbb{Z} = t_1'm_2 + t_2'm_1 + m\mathbb{Z}$, then $t_1m_2 \equiv t_1'm_2 \mod m_1$ and $t_2m_1 \equiv t_2'm_1 \mod m_2$. Since $(m_1, m_2) = 1$, we obtain $t_i \equiv t_i' \mod m_i$ for $i \in \{1, 2\}$, and thus $(t_1 + m_1\mathbb{Z}, t_2 + m_2\mathbb{Z}) = (t_1' + m_1\mathbb{Z}, t_2' + m_2\mathbb{Z})$.

2) Assume to the contrary that there exists some $(t_1, t_2) \in \mathbb{Z}^2$ such that $(t_1, m_1) = (t_2, m_2) = 1$, and yet there is some prime p dividing $(t_1m_2 + t_2m_1, m)$. As $p \,|\, m$, we may assume that $p \,|\, m_1$. Then $p \nmid t_1$, $p \nmid m_2$, but as $p \,|\, t_1m_2$, this is a contradiction. □

Theorem A.3.6 (Structure theorem for residue class rings)**.** *Let* m *be a positive integer.*

1. *If* $a \in \mathbb{Z}$, *then* $(a, m) = 1$ *if and only if* $a + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})^\times$.
2. $\mathbb{Z}/m\mathbb{Z}$ *is a field if and only if* m *is a prime.*

PROOF. 1. If $(a, m) = 1$, then there exist $x,\ y \in \mathbb{Z}$ such that $ax + my = 1$, hence $(a + m\mathbb{Z})(x + m\mathbb{Z}) = 1 + m\mathbb{Z}$, and thus $a + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})^\times$. Conversely, if $a + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})^\times$, then there is some $x \in \mathbb{Z}$ such that $(a + m\mathbb{Z})(x + m\mathbb{Z}) = 1 + m\mathbb{Z}$, and therefore $ax = 1 + my$ for some $y \in \mathbb{Z}$, which implies $(a, m) = 1$.

2. Note that $(\mathbb{Z}/m\mathbb{Z})^\bullet = \{a + m\mathbb{Z} \mid a \in [1, m-1]\}$. If m is a prime, then $(a, m) = 1$ for all $a \in [1, m-1]$, $(\mathbb{Z}/m\mathbb{Z})^\bullet = (\mathbb{Z}/m\mathbb{Z})^\times$ by 1., and thus $\mathbb{Z}/m\mathbb{Z}$ is a

field. If m is not a prime, then there is some $a \in [2, m-1]$ such that $a \,|\, m$, and then $a + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})^\bullet \setminus (\mathbb{Z}/m\mathbb{Z})^\times$. Hence $\mathbb{Z}/m\mathbb{Z}$ is not a field. □

We close this section with a probably less known result concerning homogeneous linear Diophantine equations in three variables which is used in the proof of Theorem 5.4.6.

Theorem A.3.7. *Let a, b, c be non-zero integers and $(x,y,z) \in \mathbb{Z}^3$. Then*

$$ax + by + cz = 0$$

holds if and only if there exists some $(U,V,W) \in \mathbb{Z}^3$ such that

$$x = \frac{b}{(a,b)}V - \frac{c}{(a,c)}W\,, \quad y = \frac{c}{(b,c)}U - \frac{a}{(a,b)}V \quad \textit{and} \quad z = \frac{a}{(a,c)}W - \frac{b}{(b,c)}U\,.$$

Proof. If $(U,V,W) \in \mathbb{Z}^3$, then clearly

$$a\Big(\frac{b}{(a,b)}V - \frac{c}{(a,c)}W\Big) + b\Big(\frac{c}{(b,c)}U - \frac{a}{(a,b)}V\Big) + c\Big(\frac{a}{(a,c)}W - \frac{b}{(b,c)}U\Big) = 0\,.$$

To prove the converse, let $\boldsymbol{x} = (x,y,z)^{\mathsf{t}} \in \mathbb{Z}^3$ be such that $ax + by + cz = 0$. We may assume that $(a,b,c) = 1$, and we set $d = (a,b)$. Then $(d,c) = 1$, and there exist s, t, u, $v \in \mathbb{Z}$ such that $d = as + bt$ and $1 = du + cv$. We consider the matrix

$$A = \begin{pmatrix} b/d & s & 0 \\ -a/d & t & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & c & u \\ 0 & -d & v \end{pmatrix} = \begin{pmatrix} b/d & sc & su \\ -a/d & tc & tu \\ 0 & -d & v \end{pmatrix}.$$

Since

$$\det(A) = \Big(\frac{bt}{d} + \frac{as}{d}\Big)(du + cv) = 1\,,$$

it follows that $A \in \mathsf{SL}_2(\mathbb{Z})$, and we obtain

$$0 = ax + by + cz = (a,b,c)\, AA^{-1}\boldsymbol{x} = (0,0,1)\, A^{-1}\boldsymbol{x}\,.$$

Hence there exist λ, $\mu \in \mathbb{Z}$ such that

$$A^{-1}\boldsymbol{x} = \begin{pmatrix} \lambda \\ \mu \\ 0 \end{pmatrix}, \quad \text{and therefore } \boldsymbol{x} = \begin{pmatrix} x \\ y \\ z \end{pmatrix} = A \begin{pmatrix} \lambda \\ \mu \\ 0 \end{pmatrix} = \lambda \begin{pmatrix} \frac{b}{d} \\ -\frac{a}{d} \\ 0 \end{pmatrix} + \mu \begin{pmatrix} sc \\ tc \\ -d \end{pmatrix}.$$

If $U = (b,c)\,t\mu$, $V = \lambda$ and $W = -(a,c)\,s\mu$, then

$$\frac{b}{(a,b)}V - \frac{c}{(a,c)}W = \frac{b}{d}\lambda + sc\mu = x\,, \qquad \frac{c}{(b,c)}U - \frac{a}{(a,b)}V = tc\mu - \frac{a}{d}s\lambda = y$$

and

$$\frac{a}{(a,c)}W - \frac{b}{(b,c)}U = -as\mu - bt\mu = -d\mu = z\,.$$

□

A.4. Lattices

This section is devoted to linear algebra over $\mathbb{Z}$. We present the structure theory of finitely generated subgroups of a vector space over $\mathbb{Q}$ and prove the elementary divisor theorem. We do this in full generality, although in this volume only special cases (one- and two-dimensional lattices) occur. On the one hand, we feel that the general case gives more insight and is not much more complicated. On the other hand, we will use the elementary divisor theorem in the next section to prove the structure theorem for finite abelian groups.

Let V be a vector space over $\mathbb{Q}$. An (additive) subgroup M of V is called *finitely generated* if there exist some $n \in \mathbb{N}$ and $u_1, \ldots, u_n \in V$ such that

$$M = [u_1, \ldots, u_n] = \mathbb{Z}u_1 + \ldots + \mathbb{Z}u_n \,,$$

and then we denote by $\mathbb{Q}M = \mathbb{Q}u_1 + \ldots + \mathbb{Q}u_n$ the vector space generated by M. A finitely generated subgroup M of V satisfying $\mathbb{Q}M = V$ is called a *lattice* in V.

An n-tuple $\boldsymbol{u} = (u_1, \ldots, u_n) \in V^n$ is called *linearly independent* if it is linearly independent over $\mathbb{Q}$ [equivalently, if $(c_1, \ldots, c_n) \in \mathbb{Z}^n$ and $c_1u_1 + \ldots + c_nu_n = 0$, then $c_1 = \ldots = c_n = 0$]. If $(u_1, \ldots, u_n)$ is linearly independent and $M = [u_1, \ldots, u_n]$, then $(u_1, \ldots, u_n)$ is called a *basis* of M. Note that $(u_1, \ldots, u_n)$ is a basis of M if and only if the map $\theta \colon \mathbb{Z}^n \to M$, defined by $\theta(c_1, \ldots c_n) = c_1u_1 + \ldots + c_nu_n$ for all $(c_1, \ldots, c_n) \in \mathbb{Z}^n$, is an isomorphism [equivalently: Every $x \in M$ has a unique representation $x = c_1u_1 + \ldots + c_nu_n$ with coefficients $c_1, \ldots, c_n \in \mathbb{Z}$].

For $m, n \in \mathbb{N}$, an (n,m)-matrix $A = (a_{\nu,\mu})_{\nu\in[1,n]\,,\mu\in[1,m]} \in \mathsf{M}_{n,m}(\mathbb{Q})$ and an n-tuple $\boldsymbol{u} = (u_1, \ldots, u_n) \in V^n$, we define (in an obvious way)

$$\boldsymbol{u}A = \left(\sum_{\nu=1}^{n} u_\nu a_{\nu,1}, \ldots, \sum_{\nu=1}^{n} u_\nu a_{\nu,m}\right) \in V^m \,.$$

It is easily seen that this extended matrix multiplication satisfies all reasonable associative and distributive laws. If $\boldsymbol{u}$ is linearly independent and A, $B \in \mathsf{M}_{n,m}(\mathbb{Q})$, then $\boldsymbol{u}A = \boldsymbol{u}B$ implies $A = B$.

Lemma A.4.1. *Let V be a vector space over $\mathbb{Q}$, $n, m \in \mathbb{N}$, M a subgroup of V, $\boldsymbol{u} = (u_1, \ldots, u_n) \in M^n$ a basis of M and $\boldsymbol{v} = (v_1, \ldots, v_m) \in (\mathbb{Q}M)^m$. Then there exists a unique matrix $A \in \mathsf{M}_{n,m}(\mathbb{Q})$ such that $\boldsymbol{v} = \boldsymbol{u}A$, and the following assertions hold:*

1. *$\{v_1, \ldots, v_m\} \subset M$ if and only if $A \in \mathsf{M}_{n,m}(\mathbb{Z})$;*
2. *$\boldsymbol{v}$ is a basis of M if and only if $m = n$ and $A \in \mathsf{GL}_n(\mathbb{Z})$.*

Proof. Since $\boldsymbol{u}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}M$, it follows that for every $\mu \in [1, m]$, there exists a unique n-tuple $(a_{\mu,1}, \ldots, a_{\mu,n}) \in \mathbb{Q}^n$ such that $v_\mu = u_1a_{1,\mu} + \ldots + u_na_{n,\mu}$, and we obtain $\boldsymbol{v} = \boldsymbol{u}A$, where each column of $A = (a_{\nu,\mu})_{\nu\in[1,n],\,\mu\in[1,m]} \in \mathsf{M}_{n,m}(\mathbb{Q})$ (and thus A itself) is uniquely determined.

1. Obviously, $A \in \mathsf{M}_{n,m}(\mathbb{Z})$ implies $\{v_1, \ldots, v_m\} \subset M$. On the other hand, if $\{v_1, \ldots, v_m\} \subset M$, then there exists some matrix $A' \in \mathsf{M}_{n,m}(\mathbb{Z})$ such that $\boldsymbol{v} = \boldsymbol{u}A'$, and by the linear independence of $\boldsymbol{u}$ we obtain $A' = A$.

2. If $\boldsymbol{v}$ is a basis of M, then $\boldsymbol{u}$ and $\boldsymbol{v}$ are both $\mathbb{Q}$-bases of $\mathbb{Q}M$. Hence we get $m = n$, $\boldsymbol{u} = \boldsymbol{v}A'$ for some $A' \in \mathsf{M}_n(\mathbb{Q})$, and by 1. it follows that $A,\, A' \in \mathsf{M}_n(\mathbb{Z})$. Consequently, $\boldsymbol{u} = \boldsymbol{u}AA'$, and therefore (again by the linear independence of $\boldsymbol{u}$) $AA' = I_n$ and $A \in \mathsf{GL}_n(\mathbb{Z})$.

If $m = n$ and $A \in \mathsf{GL}_n(\mathbb{Z})$, then $A^{-1} \in \mathsf{M}_n(\mathbb{Z})$, and since $\boldsymbol{u} = \boldsymbol{v}A^{-1}$, it follows that $M = [u_1, \ldots, u_n] \subset [v_1, \ldots, v_n] \subset M$. Hence $M = [v_1, \ldots, v_n]$, and since $\boldsymbol{u}$ and $\boldsymbol{v}$ both generate the vector space $\mathbb{Q}M$, it follows that $\boldsymbol{v}$ is linearly independent. ☐

Theorem A.4.2 (Structure theorem for lattices)**.** *Let V be a finite-dimensional vector space over $\mathbb{Q}$, $\dim_{\mathbb{Q}}(V) = n$ and M a lattice in V.*

1. *M has a basis consisting of n elements.*
2. *If M' is a subgroup of M, then M' is also finitely generated. More precisely, the following holds:*

   > *There exist a basis $(u_1, \ldots, u_n)$ of M, an integer $m \in [0, n]$ and positive integers $d_1, \ldots, d_m$ such that $d_1 \,|\, d_2 \,|\, \ldots \,|\, d_m$, and $(d_1u_1, \ldots, d_mu_m)$ is a basis of M'.*

3. *For every finitely generated subgroup M' of V there exists some $d \in \mathbb{N}$ such that $dM' \subset M$.*
4. *Let M' be another lattice of V such that $M' \subset M$. Let $\boldsymbol{u} \in M^n$ be a basis of M, $\boldsymbol{u}' \in M'^n$ a basis of M' and $A \in \mathsf{M}_n(\mathbb{Z})$ such that $\boldsymbol{u}' = \boldsymbol{u}A$. Then $(M\!:\!M') = |\det(A)|$.*

Proof. We start with the proof of 3. Then we prove 2. under the assumption that M has a basis, and after this we shall deduce 1. Throughout, we tacitly apply Lemma A.4.1.

3. Let $k,\, m \in \mathbb{N}$ be such that $M = [u_1, \ldots, u_k]$ and $M' = [v_1, \ldots, v_m]$. For $j \in [1, m]$, we have $v_j \in V = \mathbb{Q}M = \mathbb{Q}u_1 + \ldots + \mathbb{Q}u_k$, and therefore there exist $b_{1,j}, \ldots, b_{k,j} \in \mathbb{Q}$ such that $v_j = b_{1,j}u_1 + \ldots + b_{k,j}u_k$. If $d \in \mathbb{N}$ is such that $db_{i,j} \in \mathbb{Z}$ for all $i \in [1, k]$ and $j \in [1, m]$, then $dv_j \in M$ for all $j \in [1, m]$, and thus $dM' \subset M$.

2. (assuming that M has a basis consisting of n elements). We may assume that $M' \neq \{0\}$, and we proceed by induction on n. For $n = 0$ there is nothing to do.

$n \geq 1$, $n - 1 \to n$: Let $d_1 \in \mathbb{N}$ be minimal such that there exist a basis $(v_1, \ldots, v_n)$ of M and $c_2, \ldots, c_n \in \mathbb{Z}$ satisfying $d_1v_1 + c_2v_2 + \ldots + c_nv_n \in M'$. For $i \in [1, n]$, suppose that $c_i = d_1q_i + r_i$, where $q_i \in \mathbb{Z}$ and $r_i \in [0, d_1 - 1]$. If $u_1 = v_1 + q_2v_2 + \ldots + q_nv_n$, then $(u_1, v_2, \ldots, v_n)$ is a basis of M and

$$d_1u_1 + r_2v_2 + \ldots + r_nv_n = d_1v_1 + c_2v_2 + \ldots + c_nv_n \in M'\,.$$

By the minimal choice of d_1 it follows that $r_i = 0$ for all $i \in [2, n]$, and consequently $d_1u_1 \in M'$.

Now we set $M_1 = [v_2, \ldots, v_n]$ and $M_1' = M' \cap M_1$. Then $(v_2, \ldots, v_n)$ is a basis of M_1, and by the induction hypothesis, there exist a basis $(u_2, \ldots, u_n)$ of M_1, some $m \in [1, n]$ and $d_2, \ldots, d_m \in \mathbb{N}$ such that $d_2 \,|\, d_3 \,|\, \ldots \,|\, d_m$, and $(d_2u_2, \ldots, d_mu_m)$ is a basis of M_1'. We assert that $(u_1, \ldots, u_n)$ is a basis of M. This is obvious if $n = 1$;

if $n \ge 2$, then $(u_2, \ldots, u_n) = (v_2, \ldots, v_n)A'$ for some matrix $A' \in \mathsf{GL}_{n-1}(\mathbb{Z})$,

$$(u_1, u_2, \ldots, u_n) = (u_1, v_2, \ldots, v_n) \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & A' \end{pmatrix}, \quad \text{and since} \quad \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & A' \end{pmatrix} \in \mathsf{GL}_n(\mathbb{Z}),$$

it follows that $(u_1, \ldots, u_n)$ is a basis of M.

It remains to prove that $M' = [d_1u_1,\, d_2u_2, \ldots, d_mu_m]$ and $d_1 \,|\, d_2$ if $m \ge 2$. Clearly, $M' \supset [d_1u_1,\, d_2u_2, \ldots, d_mu_m]$. Thus let $x = b_1u_1 + \ldots + b_nu_n \in M'$, where $b_1, \ldots, b_n \in \mathbb{Z}$, and set $b_1 = qd_1 + r$ for some $q \in \mathbb{Z}$ and $r \in [0, d_1 - 1]$. Then $x - qd_1u_1 = r_1u_1 + b_2u_2 + \ldots + b_nu_n \in M'$, hence $r = 0$ by the minimal choice of d_1, $x - qd_1u_1 \in M_1' = [d_2u_2, \ldots, d_mu_m]$ and thus $x \in [d_1u_1,\, d_2u_2, \ldots, d_mu_m]$. Assume finally that $m \ge 2$ and $d_2 = d_1q + r$ for some $q, r \in \mathbb{N}_0$ and $r < d_1$. Then $(u_1 + qu_2, u_2, \ldots, u_n)$ is a basis of M and $d_1u_1 + d_2u_2 = d_1(u_1 + qu_2) + ru_2 \in M'$. Again, the minimal choice of d_1 implies $r = 0$ and thus $d_1 \,|\, d_2$.

1. Let $(u_1, \ldots, u_n) \in M^n$ be a $\mathbb{Q}$-basis of V, $M_0 = [u_1, \ldots, u_n]$, $k \ge n$ and $u_{n+1}, \ldots, u_k \in M$ such that $M = [u_1, \ldots, u_k]$. Then $M \subset V = \mathbb{Q}M_0$, and by 3. there exists some $d \in \mathbb{N}$ such that $dM \subset M_0$. Hence $M \subset d^{-1}M_0$, and since $(d^{-1}u_1, \ldots, d^{-1}u_n)$ is a basis of $d^{-1}M_0$, it follows from 2. that the subgroup M of $d^{-1}M_0$ contains a basis $(v_1, \ldots, v_m)$ for some $m \in [0, n]$, and finally we obtain $m = \dim_{\mathbb{Q}} \mathbb{Q}M = n$.

4. By 2., there exist $d_1, \ldots, d_n \in \mathbb{N}$ and a basis $\boldsymbol{v} = (v_1, \ldots, v_n)$ of M such that $\boldsymbol{v}' = (d_1v_1, \ldots, d_nv_n)$ is a basis of M'. Hence there is an isomorphism

$$\phi\colon \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_n\mathbb{Z} \ \to\ M/M',$$

given by $\phi(c_1 + d_1\mathbb{Z}, \ldots, c_n + d_n\mathbb{Z}) = c_1u_1 + \ldots + c_nu_n + M'$, and consequently

$$(M : M') = |M/M'| = |\mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_n\mathbb{Z}| = d_1 \cdot \ldots \cdot d_n\,.$$

By Lemma A.4.1, there exist matrices $S, T \in \mathsf{GL}_n(\mathbb{Z})$ be such that $\boldsymbol{u} = \boldsymbol{v}S$ and $\boldsymbol{v}' = \boldsymbol{u}'T$. If $D = \operatorname{diag}(d_1, \ldots, d_n)$, then $\boldsymbol{v}D = \boldsymbol{v}' = \boldsymbol{u}AT = \boldsymbol{v}SAT$, hence $D = SAT$ and therefore $(M : M') = \det(D) = \det(SAT) = |\det(A)|$, since $(M : M') > 0$ and $|\det(S)| = |\det(T)| = 1$. □

Corollary A.4.3. *Let V be a vector space over $\mathbb{Q}$, $\dim_{\mathbb{Q}}(V) = n \in \mathbb{N}$ and M a subgroup of V. Then the following assertions are equivalent:*

(a) *M is a lattice in V.*

(b) *M has a basis consisting of n elements.*

(c) *M is finitely generated, and for every $z \in V$ there is some $m \in \mathbb{N}$ such that $mz \in M$.*

(d) *M is finitely generated and contains a basis of V.*

Proof. (a) ⇒ (b) By Theorem A.4.2.1.

(b) ⇒ (c) Let $(u_1, \ldots, u_n)$ be a basis of M. Then $M = [u_1, \ldots, u_n]$, and $(u_1, \ldots, u_n)$ is a basis of V. If $z \in V$, then $z = c_1u_1 + \ldots + c_nu_n$ for some $c_1, \ldots, c_n \in \mathbb{Q}$, and if $m \in \mathbb{N}$ is such that $mc_i \in \mathbb{Z}$ for all $i \in [1, n]$, then $mz \in M$.

(c) ⇒ (d) Let $(u_1, \ldots, u_n)$ be any $\mathbb{Q}$-basis of V. For $i \in [1, n]$, and let $m_i \in \mathbb{N}$ be such that $m_iu_i \in M$. Then $(m_1u_1, \ldots, m_nu_n) \in M^n$ is a basis of V.

(d) ⇒ (a) Obvious. □

Corollary A.4.4. *Let* $M \neq \{0\}$ *be a finitely generated subgroup of* $\mathbb{Q}$. *Then* $M = m\mathbb{Z}$, *where* $m = \min(M \cap \mathbb{Q}_{>0})$.

Proof. Since $M\mathbb{Q} = \mathbb{Q}$, Theorem A.4.2.1 implies $M = d\mathbb{Z}$ for some $d \in M$, hence $M = |d|\mathbb{Z}$, and $|d| = \min(M \cap \mathbb{Q}_{>0})$. □

A.5. Finite abelian groups

The main results presented in this section are the structure theorems for finite abelian groups (Theorem A.5.4 in the multiplicative case and Theorem A.5.8 in the additive case). As a preparation for these main results, we collect some simple counting results and investigate finite cyclic groups in detail. Except in Theorem A.5.8, we use multiplicative notation.

Let G be a (multiplicative) abelian group with unit element e and $a \in G$. We denote by $\operatorname{ord}(a) = |\langle a \rangle| \in \mathbb{N} \cup \{\infty\}$ the *order* of a (in G). If $f \colon \mathbb{Z} \to G$ is defined by $f(k) = a^k$ for all $k \in \mathbb{Z}$, then f is a homomorphism, and $f(\mathbb{Z}) = \langle a \rangle$. If $\operatorname{ord}(a) = \infty$, then f is a monomorphism. If $\operatorname{ord}(a) = d \in \mathbb{N}$, then $\operatorname{Ker}(f) = d\mathbb{Z}$, and f induces an isomorphism $\mathbb{Z}/d\mathbb{Z} \overset{\sim}{\to} \langle a \rangle$. In particular, if $k \in \mathbb{Z}$, then $a^k = e$ if and only if $d \mid k$, and $d = \min\{k \in \mathbb{N} \mid a^k = e\}$. By Lagrange's theorem, $|G| = (G \colon \langle a \rangle) \operatorname{ord}(a)$, hence $\operatorname{ord}(a)$ divides $|G|$, $a^{|G|} = e$, and we call $|G| \in \mathbb{N} \cup \{\infty\}$ the *order* of G.

Suppose that $a \in G$, $n \in \mathbb{N}$ and $a^n = e$. If $k \in \mathbb{Z}$, then a^k only depends on the residue class $\kappa = k + n\mathbb{Z}$, and we set $a^\kappa = a^k$. With this definition, we obtain $a^{\kappa+\lambda} = a^\kappa a^\lambda$ and $(a^\kappa)^\lambda = a^{\kappa\lambda}$ for all $\kappa, \lambda \in \mathbb{Z}/n\mathbb{Z}$. Moreover, if $\operatorname{ord}(a) = n$ and $\kappa, \lambda \in \mathbb{Z}/n\mathbb{Z}$, then $a^\kappa = a^\lambda$ if and only if $\kappa = \lambda$.

The following Theorem A.5.1 contains elementary properties of the orders of group elements.

Theorem A.5.1. *Let* G *be a finite (multiplicative) abelian group with unit element* e *and* $a, b \in G$.

1. *If* $(\operatorname{ord}(a), \operatorname{ord}(b)) = 1$, *then* $\operatorname{ord}(ab) = \operatorname{ord}(a)\operatorname{ord}(b)$.
2. *If* $\operatorname{ord}(a) = d \in \mathbb{N}$ *and* $k \in \mathbb{Z}$, *then*
$$\operatorname{ord}(a^k) = \frac{d}{(k,d)}\,.$$
3. *Suppose that* $n = n_1 n_2$, *where* $n_1, n_2 \in \mathbb{N}$ *and* $(n_1, n_2) = 1$. *Then* a *is an* n*-th power in* G *if and only if* a *is both an* n_1*-th power and an* n_2*-th power in* G.
4. *If* $n \in \mathbb{N}$ *and* $(\operatorname{ord}(a), n) = 1$, *then* a *is an* n*-th power in* G.

Proof. 1. Suppose that $\operatorname{ord}(a) = k$, $\operatorname{ord}(b) = l$ and $(k, l) = 1$. Then $(ab)^{kl} = e$, and we must prove that $(ab)^j = e$ implies $kl \mid j$ for all $j \in \mathbb{Z}$. Let $j \in \mathbb{Z}$ be such that $(ab)^j = e$. Then $e = (ab)^{kj} = b^{kj}$ and hence $l \mid kj$ and therefore $l \mid j$, say $j = ml$ for some $m \in \mathbb{Z}$. It follows that $e = (ab)^{ml} = a^{ml}$, hence $k \mid ml$, and therefore $k \mid m$ and $kl \mid ml = j$.

2. If $\operatorname{ord}(a) = d$ and $j \in \mathbb{Z}$, then $(a^k)^j = a^{kj} = e$ if and only if $d \,|\, kj$, but

$$d \,|\, kj \iff \frac{d}{(k,d)} \,\Big|\, \frac{k}{(k,d)}\, j \iff \frac{d}{(k,d)} \,\Big|\, j \quad \Big[\text{since} \quad \Big(\frac{k}{(k,d)}, \frac{d}{(k,d)}\Big) = 1\Big].$$

3. If a is an n-th power, then clearly a is also an n_1-th power and an n_2-th power. Thus assume that $a = x_1^{n_1} = x_2^{n_2}$ for some $x_1,\, x_2 \in G$, and let $u_1,\, u_2 \in \mathbb{Z}$ be such that $u_1n_1 + u_2n_2 = 1$. Then $a = a^{n_1u_1+n_2u_2} = (x_2^{n_2})^{n_1u_1}(x_1^{n_1})^{n_2u_2} = (x_1^{u_2}x_2^{u_1})^n$.

4. Suppose that $\operatorname{ord}(a) = d$, and let $u,\, v \in \mathbb{Z}$ be such that $du + nv = 1$. Then $a = a^{du}a^{nv} = (a^v)^n$ is an n-th power. □

Recall that a group G is called *cyclic* if $G = \langle g \rangle$ for some $g \in G$. In this case, it follows that $G \cong \mathbb{Z}$ if $\operatorname{ord}(g) = \infty$, and $G \cong \mathbb{Z}/n\mathbb{Z}$ if $\operatorname{ord}(g) = n \in \mathbb{N}$. If $G = \langle g \rangle$ and $|G| = n \in \mathbb{N}$, then $\{\langle g^{n/d} \rangle \mid d \in \mathbb{N},\ d \,|\, n\}$ is the set of all subgroups of G. If $d \in \mathbb{N}$ and $d \,|\, n$, then $|\langle g^{n/d} \rangle| = d$, and $\langle g^{n/d} \rangle$ is the only subgroup of order d.

Theorem A.5.2. *Let G be a finite cyclic group of order n with unit element e, $d \in \mathbb{N}$ and $a \in G$.*

1. *a is a d-th power in G if and only if $a^{n/(n,d)} = e$.*
2. *If a is a d-th power in G, then $|\{x \in G \mid x^d = a\}| = (n,d)$. In particular, $|\{x \in G \mid x^d = e\}| = (n,d)$.*
3. *G has an element of order d if and only if $d \,|\, n$, and if a is an element of order d, then $\{a^j \mid j \in [0, d-1],\ (j,d) = 1\}$ is the set of all elements of order d in G.*
4. *Let s be the product of all elements of G. Then $s = e$ if and only if n is odd, and $s^2 = e$ if n is even.*

Proof. Assume that $G = \langle g \rangle$.

1. If $a = x^d$ for some $x \in G$, then $a^{n/(n,d)} = (x^n)^{d/(n,d)} = e$. As to the converse, suppose that $a = g^k$, where $k \in [0, n-1]$, and $a^{n/(n,d)} = e$. Then $g^{kn/(n,d)} = e$, hence

$$n \,\Big|\, \frac{kn}{(n,d)}, \quad \text{and therefore} \quad (n,d) \,|\, k\,.$$

If $u,\, v \in \mathbb{Z}$ are such that $k = nu + dv$, then $a = g^k = (g^v)^d$.

2. Suppose that there is some $x_0 \in G$ such that $x_0^d = a$. If $x \in G$, then $x^d = a$ if and only if $(x_0^{-1}x)^d = e$, and therefore

$$|\{x \in G \mid x^d = a\}| = |\{z \in G \mid z^d = e\}| = |\{k \in [0, n-1] \mid g^{kd} = e\}| = (n,d)\,.$$

Indeed, if $k \in [0, n-1]$, then $g^{kd} = e$ if and only if $n \,|\, kd$, and

$$\begin{aligned} n \,|\, kd \iff \frac{n}{(n,d)} \,\Big|\, k\,\frac{d}{(n,d)} &\iff \frac{n}{(n,d)} \,\Big|\, k \\ &\iff k = \frac{nj}{(n,d)} \quad \text{for some} \quad j \in [0, (n,d)-1]\,. \end{aligned}$$

3. G has an element of order d if and only if G has a subgroup of order d, and this holds if and only if $d \,|\, n$. If a is an element of order d, then

$$\{x \in G \mid \operatorname{ord}(x) = d\} = \{x \in G \mid \langle x \rangle = \langle a \rangle\} = \{a^j \mid j \in [0, d-1],\ (j,d) = 1\}\,.$$

4. We have

$$s = \prod_{i=0}^{n-1} g^i = g^t\,, \quad \text{where} \quad t = \sum_{i=0}^{n-1} i = \frac{n(n-1)}{2}\,.$$

Now the assertion follows since $n \,|\, 2t$, and $n \,|\, t$ if and only if n is odd. □

Corollary A.5.3. *Let p be a prime, $k,\ l,\ N \in \mathbb{N}$, G a cyclic group of order p^N with unit element e, $a,\, b \in G \setminus \{e\}$ and $a = b^{p^l}$. Then b is a p^k-th power in G if and only if a is a p^{k+l}-th power in G.*

Proof. Suppose that $\operatorname{ord}(b) = p^m$ for some $m \in [0, N]$. Since $a = b^{p^l} \ne e$, it follows that $m > l$, and $\operatorname{ord}(a) = p^{m-l}$ by Theorem A.5.1.2. If $b = c^{p^k}$ for some $c \in G$, then $a = b^{p^l} = c^{p^{l+k}}$. Thus assume that a is a p^{k+l}-th power. Then $N > k+l$, by Theorem A.5.2.1 we obtain $a^{p^{N-k-l}} = e$, hence $N-k-l \ge m-l$, and therefore $m \le N-k$. Consequently, it follows that $b^{p^{N-k}} = e$, and thus b is a p^k-th power. □

Now we depart from the cyclic case and consider arbitrary finite abelian groups. The following structure theorem shows that every finite abelian group can be composed by its cyclic components.

Let G be a multiplicative finite abelian group and $r \in \mathbb{N}$. For $i \in [1, r]$, let $g_i \in G$ be such that $\operatorname{ord}(g_i) = d_i \ge 2$, and consider the cyclic subgroup $G_i = \langle g_i \rangle$ of G. Then it is easily seen that the following assertions are equivalent:

(a) Every $a \in G$ has a unique representation in the form $a = g_1^{k_1} \cdot \ldots \cdot g_r^{k_r}$, where $k_i \in [0, d_i - 1]$ for all $i \in [1, r]$.

(b) The map $G_1 \times \ldots \times G_r \to G$, defined by $(a_1, \ldots, a_r) \mapsto a_1 \cdot \ldots \cdot a_r$, is an isomorphism.

(c) There exists an isomorphism $\Phi\colon \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z} \overset{\sim}{\to} G$ such that

$$\Phi(k_1 + d_1\mathbb{Z}, \ldots, k_r + d_r\mathbb{Z}) = g_1^{k_1} \cdot \ldots \cdot g_r^{k_r} \quad \text{for all } (k_1, \ldots, k_r) \in \mathbb{Z}^r.$$

If these conditions are fulfilled, then $|G| = d_1 \cdot \ldots \cdot d_r$, and $(g_1, \ldots, g_r)$ is called a *basis* of G. For $n = 0$, we agree that the empty sequence is a basis of the trivial group $G = \{e\}$.

Theorem A.5.4 (Structure theorem for finite abelian groups)**.** *Let G be a finite (multiplicative) abelian group with unit element e. Then there exist uniquely determined integers $r \in \mathbb{N}_0$ and $d_1, \ldots, d_r \in \mathbb{N}$ such that $1 < d_1 \,|\, d_2 \,|\, \ldots \,|\, d_r$ and G has a basis $(g_1, \ldots, g_r)$ satisfying $\operatorname{ord}(g_i) = d_i$ for all $i \in [1, r]$.*

Proof. We may assume that $|G| > 1$ (otherwise we set $r = 0$).

Existence: Let $r \in \mathbb{N}$ be minimal such that G is generated by r elements, say $G = \langle h_1, \ldots, h_r \rangle$, and define $\phi\colon \mathbb{Z}^r \to G$ by $\phi(n_1, \ldots, n_r) = h_1^{n_1} \cdot \ldots \cdot h_r^{n_r}$. Then ϕ is an epimorphism and induces an isomorphism $\phi^*\colon \mathbb{Z}^r/\operatorname{Ker}(\phi) \overset{\sim}{\to} G$. By Theorem A.4.2.2 there exist a basis $(\boldsymbol{u}_1, \ldots, \boldsymbol{u}_r)$ of $\mathbb{Z}^r$, an integer $r' \in [0, r]$ and positive integers $d_1, \ldots, d_{r'}$ such that $d_1 \,|\, d_2 \,|\, \ldots \,|\, d_{r'}$ and $\operatorname{Ker}(\phi) = [d_1\boldsymbol{u}_1, \ldots, d_{r'}\boldsymbol{u}_{r'}]$. For $i \in [1, r]$, let $g_i = \phi(\boldsymbol{u}_i)$. Then $G = \langle g_1, \ldots, g_r \rangle$, $\operatorname{ord}(g_i) = d_i$ for all $i \in [1, r']$, and $\operatorname{ord}(g_i) = \infty$ for all $i \in [r'+1, r]$. By the minimal choice of r and since G is finite, it follows that $r' = r$ and $d_1 > 1$. Since every $x \in \mathbb{Z}^r/\operatorname{Ker}(\phi)$ has a unique representation $x = k_1\boldsymbol{u}_1 + \ldots + k_r\boldsymbol{u}_r + \operatorname{Ker}(\phi)$, where $k_i \in [0, d_i - 1]$ for all $i \in [1, r]$, the assertion follows.

Uniqueness: We proceed by induction on $|G|$ and suppose that uniqueness holds for all groups G' such that $|G'| < |G|$. Let $r, s, d_1, \ldots, d_r, f_1, \ldots, f_s \in \mathbb{N}$ and $g_1, \ldots, g_r, h_1, \ldots, h_s \in G$ be such that $1 < d_1 \mid d_2 \mid \ldots \mid d_r$, $1 < f_1 \mid f_2 \mid \ldots \mid f_s$, $\operatorname{ord}(g_i) = d_i$ for all $i \in [1, r]$, $\operatorname{ord}(h_j) = f_j$ for all $j \in [1, s]$, and every $a \in G$ has unique representations $a = g_1^{k_1} \cdot \ldots \cdot g_r^{k_r} = h_1^{l_1} \cdot \ldots \cdot h_s^{l_s}$, where $k_i \in [0, d_i - 1]$ for all $i \in [1, r]$, and $l_j \in [0, f_j - 1]$ for all $j \in [1, s]$. Then $|G| = d_1 \cdot \ldots \cdot d_r = f_1 \cdot \ldots \cdot f_s$.

For every prime p, the set $G^p = \{g^p \mid g \in G\}$ is a subgroup of G, and if $g \in G$ and $\operatorname{ord}(g) = d$, then

$$\operatorname{ord}(g^p) = \frac{d}{(d, p)}\,.$$

If $a \in G$, then $a^p = g_1^{k_1'} \cdot \ldots \cdot g_r^{k_r'} = h_1^{l_1'} \cdot \ldots \cdot h_s^{l_s'}$ with uniquely determined exponents

$$k_i' \in \Big[0, \ \frac{d_i}{(d_i, p)} - 1\Big] \ \text{ for all } \ i \in [1, r]\,, \quad \text{and} \quad l_j' \in \Big[0, \ \frac{f_j}{(f_j, p)} - 1\Big] \ \text{ for all } \ j \in [1, s]\,.$$

Hence it follows that

$$|G^p| = \prod_{i=1}^{r} \frac{d_i}{(p, d_i)} = \prod_{j=1}^{s} \frac{f_j}{(p, f_j)}\,,$$

and

$$\frac{|G|}{|G^p|} = p^t\,, \quad \text{where } \ t = \big|\big\{i \in [1, r] \ \big| \ p \mid d_i\big\}\big| = \big|\big\{j \in [1, s] \ \big| \ p \mid f_j\big\}\big| \le \min\{r, s\}\,.$$

In particular, for $p \mid d_1$ we obtain $r \le s$, and for $p \mid f_1$ we obtain $s \le r$. Hence it follows that $r = s$, and d_1 and f_1 are divisible by the same primes.

Let p be a prime such that $p \mid d_1$. Let $\rho, \sigma \in [0, r]$ be such that $d_i = f_j = p$ for all $i \in [1, \rho]$ and $j \in [1, \sigma]$, $d_i \ne p$ for all $i \in [\rho+1, r]$ and $f_j \ne p$ for all $j \in [\sigma+1, s]$. Then we obtain, for every $a \in G$,

$$a^p = g_{\rho+1}^{pk'_{\rho+1}} \cdot \ldots \cdot g_r^{pk_r'} = h_{\sigma+1}^{pl'_{\sigma+1}} \cdot \ldots \cdot h_r^{pl_r'}$$

with uniquely determined exponents

$$k_i' \in \Big[0, \frac{d_i}{p} - 1\Big] \ \text{ for all } \ i \in [\rho+1, r]\,, \quad \text{and} \quad l_j' \in \Big[0, \ \frac{f_j}{p} - 1\Big] \ \text{ for all } \ j \in [\sigma+1, r]\,.$$

Since $1 < \operatorname{ord}(g_{\rho+1}^p) \mid \ldots \mid \operatorname{ord}(g_r^p)$ and $1 < \operatorname{ord}(h_{\sigma+1}^p) \mid \ldots \mid \operatorname{ord}(h_r^p)$, the induction hypothesis (applied for G^p) shows that $\rho = \sigma$, and

$$\frac{d_i}{p} = \operatorname{ord}(g_i^p) = \operatorname{ord}(h_i^p) = \frac{f_i}{p} \quad \text{for all } i \in [\rho+1, r]\,.$$

Hence it follows that $d_i = f_i$ for all $i \in [1, r]$. ☐

It is possible to refine the structure theorem for finite abelian groups by focusing on the various primes dividing the group order. To do this, let again G be a finite abelian multiplicative group and p a prime. Then we define

$$G_p = \{a \in G \mid \operatorname{ord}(a) \text{ is a } p\text{-power}\} \quad \text{and} \quad G[p] = \{a \in G \mid a^p = e\} \subset G_p\,.$$

G_p and $G[p]$ are subgroups of G of p-power order, and if $|G[p]| = p^{\mathsf{r}_p(G)}$, then we call G_p the *p-component* and $\mathsf{r}_p(G)$ the *p-rank* of G. If $G = G_p$, then G is called a *p-group*, and if $G = G[p]$, then G is called an *elementary p-group.* Note that every elementary p-group is a vector space over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ in a natural way.

Corollary A.5.5. *Let G be a finite (multiplicative) abelian group and p a prime. Let $(g_1, \ldots, g_r)$ be a basis of G, and suppose that $\operatorname{ord}(g_i) = p^{\delta_i} c_i$, where $\delta_i \in \mathbb{N}_0$, $c_i \in \mathbb{N}$ and $p \nmid c_i$ for all $i \in [1, r]$. Let $l \in [0, r]$ be such that $\delta_i > 0$ if $i \in [1, l]$ and $\delta_i = 0$ if $i \in [l+1, r]$. Then*

- $(g_1^p, \ldots, g_l^p, g_{l+1}, \ldots, g_r)$ *is a basis of* G^p,
- $(g_1 G^p, \ldots, g_l G^p)$ *is a basis of* G/G^p,
- $(g_1^{c_1}, \ldots, g_l^{c_l})$ *is a basis of* G_p, *and*
- $(g_1^{c_1 p^{\delta_1 - 1}}, \ldots, g_l^{c_l p^{\delta_l - 1}})$ *is a basis of* $G[p]$.

In particular, $\mathsf{r}_p(G) = l$, $|G_p| = p^{\delta_1 + \ldots + \delta_l} = p^{\mathsf{v}_p(|G|)}$, $G[p]$ and G/G^p are vector spaces over $\mathbb{F}_p$, and $\dim_{\mathbb{F}_p}(G[p]) = \dim_{\mathbb{F}_p}(G/G^p) = \mathsf{r}_p(G)$.

Proof. Obvious by Theorem A.5.4. □

The following theorem deals with the behavior of the p-component under group homomorphisms.

Theorem A.5.6. *Let $\theta \colon G \to G'$ be an epimorphism of finite abelian groups, and let p be a prime. Then $\theta(G_p) = G'_p$, and if $p \nmid |\operatorname{Ker}(\theta)|$, then $\theta \,|\, G_p \colon G_p \to G'_p$ is an isomorphism.*

Proof. Let G and G' be multiplicative groups with unit elements $e \in G$ and $e' \in G'$. If $a \in G_p$, then $a^{p^k} = e$ for some $k \in \mathbb{N}$, hence $\theta(a)^{p^k} = \theta(a^{p^k}) = e'$, and therefore $\theta(a) \in G'_p$. Conversely, assume that $u \in G'_p$, $a \in G$, $\theta(a) = u$, $\operatorname{ord}(u) = p^k$ and $\operatorname{ord}(a) = p^l m$, where $k, l \in \mathbb{N}_0$, $m \in \mathbb{N}$ and $p \nmid m$. Then there exist $s, t \in \mathbb{Z}$ such that $ms + p^k t = 1$, and we obtain $(a^{ms})^{p^l} = (a^{p^l m})^s = e$, hence $a^{ms} \in G_p$ and $\theta(a^{ms}) = u^{ms} = u^{1 - p^k t} = u \in \theta(G_p)$.

If $p \nmid |\operatorname{Ker}(\theta)|$, then $\operatorname{Ker}(\theta \,|\, G_p) = \operatorname{Ker}(\theta) \cap G_p = \{e\}$, and $\theta \,|\, G_p \colon G_p \to G'_p$ is an isomorphism. □

Theorem A.5.7. *If K is a field, then every finite subgroup G of $K^\times$ is cyclic. In particular, if K is a finite field, then $K^\times$ is cyclic.*

Proof. Let K be a field, and assume to the contrary that there is a finite subgroup G of $K^\times$ which is not cyclic. By Theorem A.5.4, there exist integers $r \geq 2$ and $d_1, \ldots, d_r \in \mathbb{N}$ satisfying $1 < d_1 \mid d_2 \mid \ldots \mid d_r$, and G has a basis $(g_1, \ldots, g_r)$ such that $\operatorname{ord}(g_i) = d_i$ for all $i \in [1, r]$. If p is a prime such that $p \mid d_1$, then we obtain $\langle g_1^{d_1/p}, g_2^{d_2/p}\rangle \subset \{x \in K \mid x^p = 1\}$, and since $|\langle g_1^{d_1/p}, g_2^{d_2/p}\rangle| = p^2$, it follows that the polynomial $X^p - 1$ has p^2 zeros in K, a contradiction. □

Because of its importance, we rephrase the essential statement of Theorem A.5.4 for additive abelian groups.

Theorem A.5.8 (Structure theorem for finite additive abelian groups)**.** *Let G be an additive finite abelian group.*

1. *There exist uniquely determined integers $r \in \mathbb{N}_0$ and $d_1, \ldots, d_r \in \mathbb{N}$ such that $1 < d_1 \mid d_2 \mid \ldots \mid d_r$ and there is an isomorphism $G \xrightarrow{\sim} \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z}$.*
2. *For $m \in \mathbb{Z}$, the multiplication $\mu_m \colon G \to G$, given by $\mu_m(x) = mx$ for all $x \in G$, is bijective if and only if $(m, |G|) = 1$.*

Proof. 1. By Theorem A.5.4.

2. Assume first that $(m, |G|) = 1$, and let $u, v \in \mathbb{Z}$ be such that $mu + |G|v = 1$. If $x \in G$, then $x = (mu + |G|v)x = m(ux)$. Hence μ_m is surjective and thus bijective. Conversely, suppose that there is some prime p such that $p \mid (m, |G|)$. By 1., there exists some element $g \in G$ such that $\operatorname{ord}(g) = p$, and then $mg = 0$. Hence μ_m is not injective. □

A.6. Prime residue class groups

In this section we apply our results on finite abelian groups to determine the structure of the *prime residue class groups* $(\mathbb{Z}/m\mathbb{Z})^\times$.

If $m, n \in \mathbb{N}$ and $m \mid n$, then $n\mathbb{Z} \subset m\mathbb{Z}$, and thus there is a natural ring epimorphism $\pi_{n,m} \colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, given by $\pi_{n,m}(a + n\mathbb{Z}) = a + m\mathbb{Z}$ for all $a \in \mathbb{Z}$. It is not at all obvious that this epimorphism induces an epimorphism on the prime residue class groups.

Theorem A.6.1. *If $m, n \in \mathbb{N}$ and $m \mid n$, then $\pi_{n,m}((\mathbb{Z}/n\mathbb{Z})^\times) = (\mathbb{Z}/m\mathbb{Z})^\times$.*

Proof. Suppose that $c + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z})^\times$, where $c \in \mathbb{Z}$ and $(c, m) = 1$. We must find some $b \in \mathbb{Z}$ such that $(b, n) = 1$ and $b \equiv c \bmod m$. We set $n = mm_1q$, where m_1, $q \in \mathbb{N}$, m_1 is a product of primes dividing m, and $(q, m) = 1$. It follows that $(mm_1, q) = 1$, and by the Chinese remainder theorem there is some $b \in \mathbb{Z}$ such that $b \equiv c \bmod mm_1$ and $b \equiv 1 \bmod q$. Then it follows that $b \equiv c \bmod m$, $(b, mm_1) = (c, mm_1) = (b, q) = 1$, and thus also $(b, n) = 1$. □

Next we recall *Euler's φ function*, defined by

$$\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^\times| = |\{k \in [0, m-1] \mid (k, m) = 1\}| \quad \text{for all } m \in \mathbb{N}.$$

In particular, $\varphi(1) = 1$. If p is a prime, then $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{F}_p^\times$ is cyclic by Theorem A.5.7, and

$$\varphi(p) = |\mathbb{F}_p^\times| = p - 1\,.$$

An integer w such that $(\mathbb{Z}/p\mathbb{Z})^\times = \langle w + p\mathbb{Z}\rangle$ is called a *primitive root modulo p*.

Theorem A.6.2 (Euler's φ function)**.**

1. *If* $m_1,\ m_2 \in \mathbb{N}$ *and* $(m_1, m_2) = 1$*, then* $\varphi(m_1 m_2) = \varphi(m_1)\varphi(m_2)$*.*
2. *Suppose that* $m = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}$*, where* $r \in \mathbb{N}$*,* $p_1, \ldots, p_r$ *are distinct primes and* $e_1, \ldots, e_r \in \mathbb{N}$*. Then*
$$\varphi(m) = \prod_{i=1}^{r} p_i^{e_i-1}(p_i - 1) = m \prod_{\substack{p \in \mathbb{P} \\ p \,|\, m}} \Big(1 - \frac{1}{p}\Big)\,.$$
3. (Euler's theorem) *If* $m \in \mathbb{N}$*,* $x \in \mathbb{Z}$ *and* $(x, m) = 1$*, then* $x^{\varphi(m)} \equiv 1 \mod m$*.*
4. *If* $x \in \mathbb{R}_{>0}$ *and* $m \in \mathbb{N}$*, then*
$$|\{d \in \mathbb{N} \mid d < x,\ (d, m) = 1\}| = \frac{\varphi(m)}{m}\,x + \rho\,, \quad \textit{where} \ \ \rho \in [0, m]\,.$$

Proof. 1. Assume that $m_1,\ m_2 \in \mathbb{N}$ and $(m_1, m_2) = 1$. By the Chinese remainder theorem, there is an isomorphism $(\mathbb{Z}/m_1m_2\mathbb{Z})^\times \overset{\sim}{\rightarrow} (\mathbb{Z}/m_1\mathbb{Z})^\times \times (\mathbb{Z}/m_2\mathbb{Z})^\times$, and therefore $\varphi(m_1m_2) = |(\mathbb{Z}/m_1m_2\mathbb{Z})^\times| = |(\mathbb{Z}/m_1\mathbb{Z})^\times|\,|(\mathbb{Z}/m_2\mathbb{Z})^\times| = \varphi(m_1)\varphi(m_2)$.

2. If $m = p^e > 1$ is a prime power, then $(\mathbb{Z}/p^e\mathbb{Z})^\times = \{a + p^e\mathbb{Z} \mid a \in [1, p^e]\,,\ p \nmid a\}$, and thus $\varphi(p^e) = p^e - p^{e-1} = p^{e-1}(p - 1)$. In the general case, again the Chinese remainder theorem implies $(\mathbb{Z}/m\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{e_1}\mathbb{Z})^\times \times \ldots \times (\mathbb{Z}/p_r^{e_r}\mathbb{Z})^\times$, and
$$\varphi(m) = \prod_{i=1}^{r} \varphi(p_i^{e_i}) = \prod_{i=1}^{r} p_i^{e_i-1}(p_i - 1) = m \prod_{\substack{p \in \mathbb{P} \\ p \,|\, m}} \Big(1 - \frac{1}{p}\Big)\,.$$

3. Since $|(\mathbb{Z}/m\mathbb{Z})^\times| = \varphi(m)$, it follows that $\xi^{\varphi(m)} = 1 + m\mathbb{Z}$ for all $\xi \in (\mathbb{Z}/m\mathbb{Z})^\times$, and consequently $x^{\varphi(m)} \equiv 1 \mod m$ for all $x \in \mathbb{Z}$ such that $(x, m) = 1$.

4. Suppose that $x = gm + s$, where $g \in \mathbb{N}_0$ and $s \in [1, m]$ (division with remainder, see Section A.3). Then $|\{d \in \mathbb{N} \mid d < x,\ (d, m) = 1\}| = g\varphi(m) + s_1$, where $s_1 = |\{d \in [gm + 1, gm + \lfloor s \rfloor] \mid (d, m) = 1\}| \le s \le m$, and we obtain
$$g\varphi(m) + s_1 = (x - s)\frac{\varphi(m)}{m} + s_1 \le x\,\frac{\varphi(m)}{m} + s\Big(1 - \frac{\varphi(m)}{m}\Big) \le x\,\frac{\varphi(m)}{m} + m\,. \quad \square$$

We proceed with the quotation of some classical congruences of elementary number theory which follow by simple group-theoretical arguments.

Theorem A.6.3 (Some classical congruences)**.** *Let* p *be an odd prime.*

1. (Fermat's little theorem) If $x \in \mathbb{Z} \setminus p\mathbb{Z}$, then $x^{p-1} \equiv 1 \mod p\,.$
2. If $x \in \mathbb{Z}$ and $n \in \mathbb{N}$, then $x^{p^n} \equiv x \mod p$.
3. If $x \in \mathbb{Z} \setminus p\mathbb{Z}$, then $x^{(p-1)/2} \equiv \pm 1 \mod p$.
4. (Wilson's theorem) $(p - 1)! \equiv -1 \mod p$.
5. We have
$$\Big(\frac{p-1}{2}\Big)!^2 \equiv (-1)^{(p+1)/2} \equiv \begin{cases} -1 \mod p & \text{if} \quad p \equiv 1 \mod 4\,, \\ 1 \mod p & \text{if} \quad p \equiv 3 \mod 4\,. \end{cases}$$
6. There is some $x \in \mathbb{Z}$ such that $x^2 \equiv -1 \mod p$ if and only if $p \equiv 1 \mod 4$.

PROOF. 1. By Theorem A.6.2.3, since $\varphi(p) = p-1$.

2. Obvious by 1. and a simple induction on n.

3. If $\xi \in \mathbb{F}_p = \mathbb{Z}/pZ$ and $\xi^2 = 1 + p\mathbb{Z}$, the $\xi = \pm 1 + p\mathbb{Z}$, since $\mathbb{F}_p$ is a field. If $x \in \mathbb{Z} \setminus p\mathbb{Z}$, then $(x^{(p-1)/2})^2 = x^{p-1} \equiv 1 \bmod p$, and therefore $x^{(p-1)/2} \equiv \pm 1 \bmod p$.

4. $(p-1)! + p\mathbb{Z}$ is the product of all elements of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times$, and since $|(\mathbb{Z}/p\mathbb{Z})^\times| = p-1$ is even, the assertion follows by Theorem A.5.2.4.

5. Since

$$\Big(\frac{p-1}{2}\Big)!^2 \equiv \prod_{i=1}^{(p-1)/2} i \prod_{i=1}^{(p-1)/2} (p-i) \prod_{i=1}^{(p-1)/2} (-1) \equiv \ (p-1)!(-1)^{(p-1)/2} \mod p\,,$$

the assertion follows by 4.

6. There is some $x \in \mathbb{Z}$ such that $x^2 \equiv -1 \bmod p$ if and only if $-1 + p\mathbb{Z}$ is a square in $\mathbb{F}_p^\times$. Since $\mathbb{F}_p^\times$ is a cyclic group of order $p-1$, the assertion follows by Theorem A.5.2.1 □

Theorem A.6.4 (Structure of the prime residue class group)**.** *Let e be a positive integer.*

1. *Let p be an odd prime and $w \in \mathbb{Z}$ a primitive root modulo p. Then*

$$(\mathbb{Z}/p^e\mathbb{Z})^\times = \langle w^{p^{e-1}} + p^e\mathbb{Z},\, (1+p) + p^e\mathbb{Z}\rangle = \langle w^{p^{e-1}}(1+p) + p^e\mathbb{Z}\rangle\,.$$

In particular, $(\mathbb{Z}/p^e\mathbb{Z})^\times$ is cyclic, $(1+p)+p^e\mathbb{Z}$ has order p^{e-1} in $(\mathbb{Z}/p^e\mathbb{Z})^\times$, $w^{p^{e-1}} + p^e$ has order $p-1$ in $(\mathbb{Z}/p^e\mathbb{Z})^\times$, and

$$\langle (1+p) + p^e\mathbb{Z}\rangle = \{a + p^e\mathbb{Z} \mid a \equiv 1 \mod p\} \subset (\mathbb{Z}/p^e\mathbb{Z})^\times\,.$$

If $x \in \mathbb{Z}$, then $x^{p^{e-1}} \equiv 1 \bmod p^e$ if and only if $x \equiv 1 \bmod p$.

2. *If $e \ge 3$, then $(\mathbb{Z}/2^e\mathbb{Z})^\times = \langle -1 + 2^e\mathbb{Z},\, 5 + 2^e\mathbb{Z}\rangle$, $5 + 2^e\mathbb{Z}$ has order 2^{e-2} in $(\mathbb{Z}/2^e\mathbb{Z})^\times$, and $\langle 5 + 2^e\mathbb{Z}\rangle = \{a + 2^e\mathbb{Z} \mid a \equiv 1 \bmod 4\} \subset (\mathbb{Z}/2^e\mathbb{Z})^\times$.*

PROOF. 1. We prove first:

A. $(1+p)^{p^k} \equiv 1 + p^{k+1} \bmod p^{k+2}$ for all $k \in \mathbb{N}_0$.

Proof of **A.** We use induction on k. For $k = 0$ there is nothing to do.

$k \ge 0$, $k \to k+1$: By the induction hypothesis, there is some $u \in \mathbb{Z}$ such that $(1+p)^{p^k} = 1 + p^{k+1} + up^{k+2} = 1 + p^{k+1}(1+pu)$. Hence it follows that

$$(1+p)^{p^{k+1}} = \sum_{j=0}^{p} \binom{p}{j} p^{j(k+1)}(1+pu)^j \equiv 1 + p^{1+(k+1)}(1+pu) \equiv 1 + p^{k+2} \mod p^{k+3},$$

since $\mathsf{v}_p(p^{p(k+1)}) = p(k+1) \ge k+3$, and

$$\mathsf{v}_p\Big(\binom{p}{j} p^{j(k+1)}\Big) \ge 1 + 2(k+1) \ge k+3 \quad \text{for all } \ j \in [2, p-1].$$

Hence **A** holds, and therefore the residue class $(1+p)+p^e\mathbb{Z}$ has order p^{e-1} in $(\mathbb{Z}/p^e\mathbb{Z})^\times$. The map $\pi\colon (\mathbb{Z}/p^e\mathbb{Z})^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$, defined by $\pi(a+p^e\mathbb{Z}) = a+p\mathbb{Z}$ for all $a \in \mathbb{Z}\setminus p\mathbb{Z}$, is an epimorphism, and

$$|\mathrm{Ker}(\pi)| = \frac{|(\mathbb{Z}/p^e\mathbb{Z})^\times|}{|(\mathbb{Z}/p\mathbb{Z})^\times|} = \frac{p^{e-1}(p-1)}{p-1} = p^{e-1} = |\langle 1+p+p^e\mathbb{Z}\rangle|\,.$$

By definition, $\mathrm{Ker}(\pi) = \{a+p^e\mathbb{Z} \mid a \in \mathbb{Z}\,,\ a \equiv 1 \bmod p\} \supset \langle (1+p)+p^e\mathbb{Z}\rangle$, and therefore equality holds. If $x \in \mathbb{Z}$ and $x^{p^{e-1}} \equiv 1 \bmod p^e$, then $x \equiv x^{p^{e-1}} \equiv 1 \bmod p$. Conversely, if $x \equiv 1 \bmod p$, then $x+p^e\mathbb{Z} \in \mathrm{Ker}(\pi)$ and therefore $x^{p^{e-1}} \equiv 1 \bmod p^e$.

Since $w^p \equiv w \bmod p$, we obtain $w^{p^{e-1}j} \equiv w^j \not\equiv 1 \bmod p$ for all $j \in [1, p-2]$, and as $\varphi(p^e) = p^{e-1}(p-1)$, it follows that $w^{p^{e-1}}+p^e\mathbb{Z}$ has order $p-1$ in $(\mathbb{Z}/p^e\mathbb{Z})^\times$. By Theorem A.5.1.1, $w^{p^{e-1}}(1+p)+p^e\mathbb{Z} = (w^{p^{e-1}}+p^e\mathbb{Z})((1+p)+p^e\mathbb{Z})$ has order $p^{e-1}(p-1)$, and therefore $(\mathbb{Z}/p^e\mathbb{Z})^\times = \langle w^{p^{e-1}}(1+p)+p^e\mathbb{Z}\rangle = \langle w^{p^{e-1}}+p^e\mathbb{Z},\, (1+p)+p^e\mathbb{Z}\rangle$.

2. We prove first:

B. $5^{2^k} \equiv 1+2^{k+2} \bmod 2^{k+3}$ for all $k \in \mathbb{N}_0$.

Proof of **B.** We use induction on k. For $k=0$ there is nothing to do.

$k \geq 0\,,\ k \to k+1$: By the induction hypothesis, there is some $u \in \mathbb{Z}$ such that $5^{2^k} = 1+2^{k+2}+2^{k+3}u = 1+2^{k+2}(1+2u)$, and therefore

$$5^{2^{k+1}} = 1+2^{k+3}(1+2u)+2^{2k+4}(1+2u)^2 \equiv 1+2^{k+3} \bmod 2^{k+4}\,.$$

Hence **B** holds, and therefore the residue class $5+2^e\mathbb{Z}$ has order 2^{e-2} in $(\mathbb{Z}/2^e\mathbb{Z})^\times$. The map $\pi\colon (\mathbb{Z}/2^e\mathbb{Z})^\times \to (\mathbb{Z}/4\mathbb{Z})^\times$, defined by $\pi(a+2^e\mathbb{Z}) = a+4\mathbb{Z}$ for all $a \in \mathbb{Z}\setminus 2\mathbb{Z}$, is an epimorphism, and

$$|\mathrm{Ker}(\pi)| = \frac{|(\mathbb{Z}/2^e\mathbb{Z})^\times|}{|(\mathbb{Z}/4\mathbb{Z})^\times|} = 2^{e-2} = |\langle 5+2^e\mathbb{Z}\rangle|\,.$$

By definition, $\mathrm{Ker}(\pi) = \{a+2^e\mathbb{Z} \mid a \in \mathbb{Z}\,,\ a \equiv 1 \bmod 4\} \supset \langle 5+2^e\mathbb{Z}\rangle|$, and thus equality holds. Since the residue class $-1+2^e\mathbb{Z} \in (\mathbb{Z}/2^e\mathbb{Z})^\times \setminus \mathrm{Ker}(\pi)$ has order 2, it follows that $(\mathbb{Z}/2^e\mathbb{Z})^\times = \langle -1+2^e\mathbb{Z},\, 5+2^e\mathbb{Z}\rangle$. □

Theorem A.6.5. *Let* $m = 2^e p_1^{e_1}\cdot\ldots\cdot p_r^{e_r}$ *be a positive integer, where* $r,\ e \in \mathbb{N}_0$, $p_1,\ldots,p_r$ *are distinct odd primes,* $e_1,\ldots,e_r \in \mathbb{N}$, *and*

$$\rho = \begin{cases} r & \textit{if}\ \ e \leq 1\,, \\ r+1 & \textit{if}\ \ e = 2\,, \\ r+2 & \textit{if}\ \ e = 3\,. \end{cases}$$

For $i \in [1,r]$, *set* $d_i = p_i^{e_i-1}(p_i-1)$, *and let* $\pi_i \in \mathbb{Z}$ *be such that*

$$\langle \pi_i + p_i^{e_i}\mathbb{Z}\rangle = (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times \quad \textit{and} \quad \pi_i \equiv 1 \bmod \frac{m}{p_i^{e_i}}\,.$$

If $e \geq 2$, *set* $d_{r+1} = 2$, *and let* $\pi_{r+1} \in \mathbb{Z}$ *be such that*

$$\pi_{r+1} \equiv -1 \bmod 2^e \quad \textit{and} \quad \pi_{r+1} \equiv 1 \bmod \frac{m}{2^e}\,.$$

If $e \ge 3$, *set* $d_{r+2} = 2^{e-2}$, *and let* $\pi_{r+2} \in \mathbb{Z}$ *be such that*

$$\pi_{r+2} \equiv 5 \mod 2^e \quad \textit{and} \quad \pi_{r+2} \equiv 1 \mod \frac{m}{2^e}\,.$$

Then $(\pi_1 + m\mathbb{Z}, \ldots, \pi_\rho + m\mathbb{Z})$ *is a basis of* $(\mathbb{Z}/m\mathbb{Z})^\times$, *and* $d_i = \operatorname{ord}(\pi_i + m\mathbb{Z})$ *for all* $i \in [1, \rho]$.

Proof. By Theorem A.6.4 it follows that $d_i = \operatorname{ord}(\pi_i + m\mathbb{Z})$ for all $i \in [1, \rho]$. We must prove that, for every $a \in \mathbb{Z}$ such that $(a, m) = 1$ there exist uniquely determined $k_1, \ldots, k_\rho \in \mathbb{N}_0$ such that $a \equiv \pi_1^{k_1} \cdot \ldots \cdot \pi_\rho^{k_\rho} \mod m$ and $k_i < d_i$ for all $i \in [1, \rho]$.

If $a \in \mathbb{Z}$ and $(k_1, \ldots, k_\rho) \in \mathbb{N}_0^\rho$, then $a \equiv \pi_1^{k_1} \cdot \ldots \cdot \pi_\rho^{k_\rho} \mod m$ holds if and only if

$$a \equiv \pi_i^{k_i} \mod p_i^{e_i} \;\text{ for all }\; i \in [1, r]\,,$$

$$a \equiv (-1)^{k_{r+1}} \mod 2^e \;\text{ if }\; e \ge 2\,, \quad \text{and} \quad a \equiv 5^{k_{r+2}} \mod 2^e \;\text{ if }\; e \ge 3\,.$$

However, Theorem A.6.4 implies that for every $i \in [1, \rho]$ there exists a uniquely determined integer $k_i \in [0, d_i - 1]$ satisfying this condition. ☐

A.7. Roots of unity and characters of finite abelian groups

In this section we prove some elementary properties of roots of unity and derive the character theory of finite abelian groups, which plays a prominent role in the Chapters 4, 6, 7 and 8 of this volume.

We start with roots of unity. A complex number z is called a *root of unity* if $z^n = 1$ for some $n \in \mathbb{N}$. The set $\mathbb{W}$ of all roots of unity is a subgroup of $\mathbb{C}^\times$, and for a subring D of $\mathbb{C}$ we denote by $\mathbb{W}(D) = \mathbb{W} \cap D$ the group of roots of unity in D. In particular, $\mathbb{W}(D) = \{\pm 1\}$ if $D \subset \mathbb{R}$. For $n \in \mathbb{N}$, we denote by

$$\mathbb{W}_n = \{z \in \mathbb{C}^\times \mid z^n = 1\} = \{\mathsf{e}^{2\pi \mathsf{i} k/n} \mid k \in [0, [n-1]\,\} = \langle \mathsf{e}^{2\pi\mathsf{i}/n} \rangle \subset \mathbb{C}^\times$$

the cyclic group of all n-th roots of unity. A root of unity $\zeta \in \mathbb{W}_n$ is called a *primitive* n-th root of unity if $\operatorname{ord}(\zeta) = n$ [equivalently, $\mathbb{W}_n = \langle \zeta \rangle$]. We denote by $\mathbb{W}_n^*$ the set of all primitive n-th roots of unity.

If $z \in \mathbb{W}_n$ and $k \in \mathbb{Z}$, then z^k only depends on the residue class $\kappa = k + n\mathbb{Z}$, and (as in Section A.5) we set $z^\kappa = z^k$. If $\zeta \in \mathbb{W}_n^*$ is a fixed primitive n-th root of unity, then the assignment $\kappa \mapsto \zeta^\kappa$ defines an isomorphism $\theta\colon \mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \mathbb{W}_n$, and since

$$\operatorname{ord}(\zeta^k) = \frac{n}{(n,k)} \quad \text{for all} \quad k \in \mathbb{Z}\,,$$

we get $\mathbb{W}_n^* = \{\zeta^k \mid k \in [0, n-1],\ (n,k) = 1\,\} = \theta((\mathbb{Z}/n\mathbb{Z})^\times)$ and $|\mathbb{W}_n^*| = \varphi(n)$. Moreover, if $\zeta \in \mathbb{W}_n^*$, $d \in \mathbb{N}$ and $d \,|\, n$, then $\zeta^d \in \mathbb{W}_{n/d}^*$.

The primitive n-th root of unity $\zeta_n = \mathsf{e}^{2\pi\mathsf{i}/n} \in \mathbb{C}^\times$ is called the *normalized* primitive n-th root of unity. We have

$$\zeta_1 = 1\,, \quad \zeta_2 = -1\,, \quad \zeta_3 = \frac{-1+\sqrt{-3}}{2}\,, \quad \zeta_4 = \mathsf{i}\,, \quad \zeta_6 = \frac{1+\sqrt{-3}}{2} \quad \text{and} \quad \zeta_8 = \frac{1+\mathsf{i}}{\sqrt{2}}\,.$$

Lemma A.7.1. *Let m, $n \in \mathbb{N}$ be positive integers.*

1. *If $z \in \mathbb{W}_n$, then*

$$\sum_{k=0}^{n-1} z^k = \sum_{\kappa \in \mathbb{Z}/n\mathbb{Z}} z^\kappa = \begin{cases} n & \textit{if} \quad z = 1\,, \\ 0 & \textit{if} \quad z \neq 1\,. \end{cases}$$

2. *If $e = \mathrm{lcm}(n,m)$, then $\mathbb{W}_n\mathbb{W}_m = \mathbb{W}_e$.*

Proof. 1. If $z = 1$, this is obvious. If $z \neq 1$, the assertion follows since

$$(z-1)\sum_{k=0}^{n-1} z^k = z^n - 1 = 0\,.$$

2. Obviously, $\mathbb{W}_n\mathbb{W}_m \subset \mathbb{W}_e$. To prove the opposite inclusion, set $d = (m,n)$, and let k, $l \in \mathbb{Z}$ be such that $d = km + ln$. Then

$$\frac{1}{e} = \frac{d}{mn} = \frac{k}{n} + \frac{l}{m}\,, \quad \text{hence} \quad \zeta_e = \mathsf{e}^{2\pi \mathsf{i}/e} = (\mathsf{e}^{2\pi \mathsf{i}/n})^k (\mathsf{e}^{2\pi \mathsf{i}/m})^l = \zeta_n^k \zeta_m^l \in \mathbb{W}_n\mathbb{W}_m\,. \qquad \square$$

The following Lemma is used for the summation of Gauss sums (Theorem 3.5.7).

Lemma A.7.2. *Let p be an odd prime. Then there exists some $b_0 \in \mathbb{R}_{>0}$ such that*

$$\det(\zeta_p^{\nu\mu})_{\nu,\,\mu \in [1,p-1]} \;=\; \mathsf{i}^{p(p-1)/2} b_0\,.$$

Proof. By the well-known formula for the Vandermonde determinant, we find

$$\begin{aligned} b = \det(\zeta_p^{\nu\mu})_{\nu,\mu \in [1,p-1]} &= \zeta_p^{1+2+\ldots+(p-1)} \det\bigl(\zeta_p^{(\nu-1)\mu}\bigr)_{\nu,\mu\in[1,p-1]} \\ &= \zeta_p^{p(p-1)/2} \prod_{1 \le l < k \le p-1} (\zeta_p^k - \zeta_p^l) = \prod_{1 \le l < k \le p-1} (\zeta_p^k - \zeta_p^l)\,. \end{aligned}$$

For $1 \le l < k \le p-1$ we obtain

$$\zeta_p^k - \zeta_p^l = \zeta_{2p}^{2k} - \zeta_{2p}^{2l} = \zeta_{2p}^{k+l}(\zeta_{2p}^{k-l} - \zeta_{2p}^{l-k}) = \zeta_{2p}^{k+l}\Bigl(2\mathsf{i}\sin\frac{(k-l)\pi}{p}\Bigr)\,,$$

and therefore

$$b = \zeta_{2p}^{S_{p-1}}\, \mathsf{i}^{T_{p-1}} b_0\,, \quad \text{where} \quad b_0 = \prod_{1 \le l < k \le p-1} 2\sin\frac{(k-l)\pi}{p} \in \mathbb{R}_{>0}\,,$$

$$S_N = \sum_{1 \le l < k \le N} (k+l) \quad \text{and} \quad T_N = \sum_{1 \le l < k \le N} 1 \quad \text{for } N \in \mathbb{N}\,.$$

It follows by an easy induction on N that

$$S_N = \frac{(N+1)N(N-1)}{2} \quad \text{and} \quad T_N = \frac{N(N-1)}{2}\,.$$

Hence we obtain

$$\zeta_{2p}^{S_{p-1}}\, \mathsf{i}^{T_{p-1}} = (-1)^{(p-1)(p-2)/2}\, \mathsf{i}^{(p-1)(p-2)/2} = \mathsf{i}^{3(p-1)(p-2)/2} = \mathsf{i}^{p(p-1)/2}\,,$$

since $3(p-1)(p-2) = p^2 - p + (2p^2 - 8p + 6) \equiv p(p-1) \bmod 8$. $\square$

Now we consider group characters. Let G be a (multiplicative) finite abelian group with unit element $e \in G$ and $|G| = n$. A homomorphism $\chi\colon G \to \mathbb{C}^\times$ is called a *character* of G. Since $\chi(t)^n = \chi(t^n) = \chi(e) = 1$ for all $t \in G$, it follows that $\chi(G) \subset \mathbb{W}_n$, and $\chi(t)^{-1} = \overline{\chi(t)}$ for all $t \in G$.

For two characters χ_1, χ_2 of G, we define their product $\chi_1\chi_2\colon G \to \mathbb{C}^\times$ by $(\chi_1\chi_2)(t) = \chi_1(t)\chi_2(t)$ for all $t \in G$. Then $\chi_1\chi_2$ is again a character, and with this point-wise multiplication the set $\widehat{G}$ of all characters of G is a multiplicative abelian group, called the *character group* of G. The *unit character* or *trivial character* $\mathbf{1} \in \widehat{G}$, defined by $\mathbf{1}(t) = 1$ for all $t \in G$, is the unit element of $\widehat{G}$. For $\chi \in \widehat{G}$, its inverse $\chi^{-1} = \overline{\chi}$ is given by $\chi^{-1}(t) = \chi(t)^{-1} = \overline{\chi(t)}$ for all $t \in G$.

A character $\chi \in \widehat{G}$ is called *real* if $\chi(G) \subset \{\pm 1\}$ [equivalently, $\overline{\chi} = \chi$], and *quadratic* if $\operatorname{ord}(\chi) = 2$. By definition, χ is real if and only if $\chi^2 = \mathbf{1}$, and χ is quadratic if and only if χ is real and $\chi \neq \mathbf{1}$. In accordance with the terminology introduced after Theorem A.5.4, we denote by

$$\widehat{G}\,[2] = \{\chi \in \widehat{G} \mid \chi^2 = \mathbf{1}\}$$

the group of all real characters of G. Every real character χ induces a character (also denoted by χ) of the factor group G/G^2 by means of $\chi(gG^2) = \chi(g)$ for all $g \in G$. In this way we identify the groups $\widehat{G}\,[2]$ and $\widehat{G/G^2}$.

In the following Theorem A.7.3 we use the structure theorem for finite abelian groups to determine the structure of the character group. We prove that the character group of a finite abelian group G is isomorphic to the group itself, and from a basis of G and suitable roots of unity, we construct a basis of $\widehat{G}$. As an application, we describe in detail the group of real characters in Corollary A.7.4, and we prove the orthogonality relations for group characters (Theorem A.7.7). These are central tools for the proof of Dirichlet's theorem on primes in arithmetic progressions (in Chapter 4) and in the genus theory of binary quadratic forms (in Chapter 6).

Theorem A.7.3 (Structure theorem for group characters)**.** *Let G be a (multiplicative) finite abelian group with unit element e, $r \in \mathbb{N}$, $(g_1, \ldots, g_r)$ a basis of G and $\operatorname{ord}(g_i) = d_i$ for all $i \in [1, r]$.*

1. *The map $\Theta\colon \widehat{G} \to \mathbb{W}_{d_1} \times \ldots \times \mathbb{W}_{d_r}$, defined by $\Theta(\chi) = (\chi(g_1), \ldots, \chi(g_r))$ for all $\chi \in \widehat{G}$, is an isomorphism. In particular, $G \cong \widehat{G}$, and for every $(\zeta_1, \ldots, \zeta_r) \in \mathbb{W}_{d_1} \times \ldots \times \mathbb{W}_{d_r}$, there exists a unique character $\chi \in \widehat{G}$ such that $\chi(g_i) = \zeta_i$ for all $i \in [1, r]$.*
2. *For $i \in [1, r]$, let ζ_i be a primitive d_i-th root of unity, and let $\chi_i \in \widehat{G}$ be a character satisfying $\chi_i(g_i) = \zeta_i$ and $\chi_i(g_j) = 1$ for all $j \in [1, r] \setminus \{i\}$. Then $(\chi_1, \ldots, \chi_r)$ is a basis of $\widehat{G}$, $\operatorname{ord}(\chi_i) = d_i$ for all $i \in [1, r]$, and for every $a \in G \setminus \{e\}$ there is some $\chi \in \widehat{G}$ such that $\chi(a) \neq 1$.*

Proof. 1. Obviously, Θ is a homomorphism. If $\chi \in \operatorname{Ker}(\Theta)$, then $\chi(g_i) = 1$ for all $i \in [1, r]$, and thus $\chi = \mathbf{1}$, since $G = \langle g_1, \ldots, g_r \rangle$. Hence Θ is a monomorphism, and it remains to prove that Θ is surjective. For $(\zeta_1, \ldots, \zeta_r) \in \mathbb{W}_{d_1} \times \ldots \times \mathbb{W}_{d_r}$, define $\chi\colon G \to \mathbb{C}^\times$ by $\chi(g_1^{k_1} \cdot \ldots \cdot g_r^{k_r}) = \zeta_1^{k_1} \cdot \ldots \cdot \zeta_r^{k_r}$ for all $(k_1, \ldots, k_r) \in \mathbb{Z}^r$ (note that both sides only depend on the residue class vector $(k_1 + d_1\mathbb{Z}, \ldots, k_r + d_r\mathbb{Z})$). Then it follows that $\chi \in \widehat{G}$, and $\Theta(\chi) = (\zeta_1, \ldots, \zeta_r)$. Hence Θ is an isomorphism, and $G \cong \mathbb{Z}/d_1\mathbb{Z} \times \ldots \times \mathbb{Z}/d_r\mathbb{Z} \cong \mathbb{W}_{d_1} \times \ldots \times \mathbb{W}_{d_r} \cong \widehat{G}$.

2. For $i \in [1,r]$, there exists (by 1.) some character $\chi_i \in \widehat{G}$ such that $\chi_i(g_i) = \zeta_i$ and $\chi_i(g_j) = 1$ for all $j \in [1,r] \setminus \{i\}$. We must prove that every $\chi \in G$ has a unique representation $\chi = \chi_1^{k_1} \cdot \ldots \cdot \chi_r^{k_r}$ where $k_i \in [0, d_i - 1]$ for all $i \in [1,r]$. Thus suppose that $\chi \in \widehat{G}$.

Existence: If $i \in [1,r]$, then $\operatorname{ord}(\zeta_i) = d_i$, and therefore there is a unique integer $k_i \in [0, d_i - 1]$ such that $\chi(g_i) = \zeta_i^{k_i}$. Then $(\chi_1^{k_1} \cdot \ldots \cdot \chi_r^{k_r})(g_i) = \chi_i(g_i)^{k_i} = \zeta_i^{k_i} = \chi(g_i)$ for all $i \in [1,r]$, hence $(\chi_1^{k_1} \cdot \ldots \cdot \chi_r^{k_r})(g) = \chi(g)$ for all $g \in G$, and therefore $\chi = \chi_1^{k_1} \cdot \ldots \cdot \chi_r^{k_r}$.

Uniqueness: If $\chi = \chi_1^{k_1} \cdot \ldots \cdot \chi_r^{k_r}$, where $k_i \in [0, d_i - 1]$ for all $i \in [1,r]$, then $\chi(g_i) = (\chi_1^{k_1} \cdot \ldots \cdot \chi_r^{k_r})(g_i) = \chi_i(g_i)^{k_i} = \zeta_i^{k_i}$ for all $i \in [1,r]$, and therefore $(k_1, \ldots, k_r)$ is uniquely determined by χ.

Suppose finally that $a = g_1^{k_1} \cdot \ldots \cdot g_r^{k_r} \in G \setminus \{e\}$, where $k_i \in [0, d_i - 1]$ for all $i \in [1,r]$. Then there is some $j \in [1,r]$ such that $k_j \neq 0$, and it follows that $\chi_j(a) = \zeta_j^{k_k} \neq 1$. □

The following two corollaries deal with special cases of arithmetical interest.

Corollary A.7.4. *Let G be a (multiplicative) finite abelian group, $r \in \mathbb{N}$ and $(g_1, \ldots, g_r)$ a basis of G such that $2 \,|\, \operatorname{ord}(g_i)$ for all $i \in [1,r]$. For $i \in [1,r]$, let $\varphi_i \in \widehat{G}$ be the unique character satisfying $\varphi_i(g_i) = -1$ and $\varphi_i(g_j) = 1$ for all $j \in [1,r] \setminus \{i\}$. Then $(\varphi_1, \ldots, \varphi_r)$ is a basis of the group $\widehat{G}[2] = \widehat{G/G^2}$ of real characters, and $|\widehat{G}[2]| = (G:G^2)$.*

Proof. For $i \in [1,r]$, set $d_i = \operatorname{ord}(g_i)$, and let ζ_i be a primitive d_i-th root of unity. Let $\chi_i \in \widehat{G}$ be a character satisfying $\chi_i(g_i) = \zeta_i$ and $\chi_i(g_j) = 1$ for all $i, j \in [1,r]$ such that $i \neq j$. For $i \in [1,r]$, set $\varphi_i = \chi_i^{d_i/2}$. Then $\operatorname{ord}(\varphi_i) = 2$, and $\varphi_i \in \widehat{G}$ is the unique character satisfying $\varphi_i(g_i) = -1$ and $\varphi_i(g_j) = 1$ for all $i, j \in [1,r]$ such that $i \neq j$. Since $(\chi_1, \ldots, \chi_r)$ is a basis of $\widehat{G}$, it follows by Corollary A.5.5 that $(\varphi_1, \ldots, \varphi_r)$ is an $\mathbb{F}_2$-basis of $\widehat{G}[2]$, and $|\widehat{G}[2]| = (G:G^2)$. □

Corollary A.7.5. *Let $G = \langle g \rangle$ be a cyclic group, $|G| = n \in \mathbb{N}$ and $d \in \mathbb{N}$.*

1. *There is an isomorphism $\Theta \colon \widehat{G} \to \mathbb{W}_n$, given by $\Theta(\chi) = \chi(g)$ for all $\chi \in \widehat{G}$. In particular, for every $\zeta \in \mathbb{W}_n$, there exists a unique character $\chi \in \widehat{G}$ such that $\chi(g) = \zeta$, and then $\operatorname{ord}(\chi) = \operatorname{ord}(\zeta)$.*
2. *If $2 \,|\, n$, then G possesses a unique quadratic character φ. It is given by $\varphi(g^k) = (-1)^k$ for all $k \in \mathbb{Z}$, and $\widehat{G}[2] = \{\mathbf{1}, \varphi\}$.*

Proof. Obvious by Theorem A.5.2. □

The following Theorem A.7.6 is basic for the investigation of power residues by means of characters.

Theorem A.7.6. *Let G be a cyclic group, $|G| = n \in \mathbb{N}$, $d \in \mathbb{N}$ and $d \,|\, n$. An element $a \in G$ is a d-th power in G if and only if $\chi(a) = 1$ for some [for every] character $\chi \in \widehat{G}$ of order d.*

Proof. Obviously, if a is a d-th power in G, then $\chi(a) = 1$ for every character $\chi \in \widehat{G}$ of order d. Thus assume that $\chi(a) = 1$ for some character $\chi \in \widehat{G}$ of order d. Suppose that $G = \langle g \rangle$, $a = g^k$ for some $k \in \mathbb{N}$ and $\chi(g) = \zeta \in \mathbb{W}_d^*$ (see Corollary A.7.5). Then $\chi(a) = \zeta^k = 1$, hence $d \,|\, k$, and if $k = dm$, then $a = (g^m)^d$. □

Theorem A.7.7. *Let G be a (multiplicative) finite abelian group with unit element e and $n = |G|$. If $a \in G$ and $\psi \in \widehat{G}$, then*

$$\sum_{t \in G} \psi(t) = \begin{cases} 0 & \text{if} \quad \psi \neq \mathbf{1}\,, \\ n & \text{if} \quad \psi = \mathbf{1}\,, \end{cases} \quad \text{and} \quad \sum_{\chi \in \widehat{G}} \chi(a) = \begin{cases} 0 & \text{if} \quad a \neq e\,, \\ n & \text{if} \quad a = e\,. \end{cases}$$

Proof. For $\psi = \mathbf{1}$ and $a = e$ the assertions are obvious. If $\psi \neq \mathbf{1}$, then there is some $a \in G$ such that $\psi(a) \neq 1$. Hence we obtain

$$\sum_{t \in G} \psi(t) = \sum_{t \in G} \psi(at) = \psi(a) \sum_{t \in G} \psi(t)\,, \quad \text{and therefore} \quad \sum_{t \in G} \psi(t) = 0\,.$$

If $a \neq e$, then (by Theorem A.7.3.2) there is some $\theta \in \widehat{G}$ such that $\theta(a) \neq 1$. Hence we obtain

$$\sum_{\chi \in \widehat{G}} \chi(a) = \sum_{\chi \in \widehat{G}} (\theta\chi)(a) = \theta(a) \sum_{\chi \in \widehat{G}} \chi(a)\,, \quad \text{and therefore} \quad \sum_{\chi \in \widehat{G}} \chi(a) = 0\,.$$ □

Theorem A.7.8 (Duality theorem for finite abelian groups)**.** *Let G be a (multiplicative) finite abelian group. For $a \in G$, we define $\widehat{a} \colon \widehat{G} \to \mathbb{C}^\times$ by $\widehat{a}(\chi) = \chi(a)$ for all $\chi \in \widehat{G}$. For subgroups H of G and Γ of $\widehat{G}$ we define their orthogonal complements by*

$$H^\perp = \{\chi \in \widehat{G} \mid H \subset \mathrm{Ker}(\chi)\} \quad \text{and} \quad \Gamma^\perp = \bigcap_{\gamma \in \Gamma} \mathrm{Ker}(\gamma) \subset G\,.$$

1. *If $a \in G$, then $\widehat{a} \in \widehat{\widehat{G}}$, and the map $\omega \colon G \to \widehat{\widehat{G}}$, defined by $\omega(a) = \widehat{a}$, is an isomorphism.*

   We identify G and $\widehat{\widehat{G}}$ by means of ω.

2. *Let H be a subgroup of G and $\pi \colon G \to G/H$ the residue class homomorphism. Then there is an exact sequence of finite abelian groups*

   $$\mathbf{1} \to \widehat{G/H} \xrightarrow{\widehat{\pi}} \widehat{G} \xrightarrow{j} \widehat{H} \to \mathbf{1}\,,$$

   where $\widehat{\pi}(\theta) = \theta \circ \pi$ for all $\theta \in \widehat{G/H}$, and $j(\chi) = \chi \,|\, H$ for all $\chi \in \widehat{G}$. In particular, $\widehat{\pi}$ induces an isomorphism $\widehat{\pi} \colon \widehat{G/H} \xrightarrow{\sim} H^\perp = \mathrm{Ker}(j)$.

   We identify $\widehat{G/H}$ and $H^\perp$ by means of $\widehat{\pi}$.

3. *For subgroups H of G and Γ of $\widehat{G}$ we have $H^{\perp\perp} = H$ and $\Gamma^{\perp\perp} = \Gamma$. In particular, the assignment $H \mapsto H^{\perp}$ defines an inclusion-reversing bijective map from the set of all subgroups of G onto the set of all subgroups of $\widehat{G}$, and its inverse is given by the assignment $\Gamma \mapsto \Gamma^{\perp}$.*
4. *Let Γ be a subgroup of $\widehat{G}$ and $\gamma \in \widehat{G} \setminus \Gamma$. Then there exists some $a \in G$ such that $\chi(a) = 1$ for all $\chi \in \Gamma$ and $\gamma(a) \neq 1$.*

PROOF. 1. If $a \in G$, then $\widehat{a}(\chi_1\chi_2) = (\chi_1\chi_2)(a) = \chi_1(a)\chi_2(a) = \widehat{a}(\chi_1)\widehat{a}(\chi_2)$ for all χ_1, $\chi_2 \in \widehat{G}$, and therefore $\widehat{a} \in \widehat{\widehat{G}}$.

If a_1, $a_2 \in G$, then $\widehat{a_1 a_2}(\chi) = \chi(a_1a_2) = \chi(a_1)\chi(a_2) = \widehat{a_1}(\chi)\widehat{a_2}(\chi) = (\widehat{a_1}\widehat{a_2})(\chi)$ for all $\chi \in \widehat{G}$, hence $\widehat{a_1 a_2} = \widehat{a}_1\widehat{a}_2$, and therefore ω is a homomorphism.

If $a \in \mathrm{Ker}(\omega)$, then $\widehat{a}(\chi) = \chi(a) = 1$ for all $\chi \in \widehat{G}$, hence $a = e$ by Theorem A.7.3.2, and thus ω is a monomorphism. Since $|G| = |\widehat{G}| = |\widehat{\widehat{G}}|$, it follows that ω is an isomorphism.

2. If $\theta \in \widehat{G/H}$, then $j \circ \widehat{\pi}(\theta) = \theta \circ \pi \,|\, H = \mathbf{1}$, and if $\widehat{\pi}(\theta) = \theta \circ \pi = \mathbf{1}$, then $\theta = \mathbf{1}$. Hence $\widehat{\pi}$ is a monomorphism and $\mathrm{Im}(\widehat{\pi}) \subset \mathrm{Ker}(j)$. Conversely, if $\chi \in \mathrm{Ker}(j)$, then $H \subset \mathrm{Ker}(\chi)$, and by Theorem A.1.1 there exists some $\chi^* \in \widehat{G/H}$ such that $\chi = \chi^* \circ \pi = \widehat{\pi}(\chi^*) \in \mathrm{Im}(\widehat{\pi})$. Since

$$|\mathrm{Im}(j)| = \frac{|\widehat{G}|}{|\mathrm{Ker}(j)|} = \frac{|\widehat{G}|}{|\widehat{G/H}|} = \frac{|G|}{|G/H|} = |H|\,,$$

it follows that j is an epimorphism. Obviously, $H^{\perp} = \mathrm{Ker}(j)$, and thus $\widehat{\pi}$ induces an isomorphism $\widehat{\pi}\colon \widehat{G/H} \xrightarrow{\sim} H^{\perp}$.

3. By definition, $H \subset \{a \in G \mid \chi(a) = 1 \text{ for all } \chi \in H^{\perp}\} = H^{\perp\perp}$, and since

$$|H^{\perp}| = |\widehat{G/H}| = \frac{|G|}{|H|}\,, \quad \text{we obtain} \quad |H^{\perp\perp}| = \frac{|\widehat{G}|}{|H^{\perp}|} = \frac{|G|}{|H^{\perp}|} = |H|\,.$$

Hence it follows that $H = H^{\perp\perp}$, and (by interchanging G and Γ and observing $\widehat{\Gamma} = G$) also $\Gamma^{\perp\perp} = \Gamma$.

4. If $\Gamma_1 = \langle \Gamma \cup \{\gamma\} \rangle \subset \widehat{G}$, then $\Gamma \subsetneq \Gamma_1$ implies $\Gamma_1^{\perp} \subsetneq \Gamma^{\perp}$, and every element $a \in \Gamma^{\perp} \setminus \Gamma_1^{\perp}$ has the desired property. □

A.8. Factorization in integral domains

In this section we present the fundamentals of divisibility theory in integral domains. In particular, we focus on prime factorizations, factorial domains and the theory of the greatest common divisor.

Throughout this section, let D be an integral domain.

An element $u \in D^{\bullet}$ is called *irreducible* or an *atom* if $u \notin D^{\times}$ and if there is no factorization $u = ab$ into elements a, $b \in D \setminus D^{\times}$ [equivalently: uD is maximal among proper principal ideals of D]. The integral domain D is called *atomic* if every $a \in D^{\bullet} \setminus D^{\times}$ is a product of atoms.

An element $p \in D^\bullet$ is called a *prime element* if pD is a prime ideal of D [equivalently: If $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in D$ are such that $a_1 \cdot \ldots \cdot a_n \in pD$, then $a_i \in pD$ for some $i \in [1, n]$]. The integral domain D is called a *factorial domain* or a *unique factorization domain* if every $a \in D^\bullet \setminus D^\times$ is a product of prime elements.

In the following Theorem A.8.1 we collocate the elementary properties of these notions. They are used in Chapter 5 to study the factorization properties of quadratic orders.

Theorem A.8.1. *Let D be an integral domain.*

1. *If $a, b \in D$, then $aD = bD$ if and only if $a = be$ for some $e \in D^\times$. In particular, if $u \in D$ and $e \in D^\times$, then u is an atom [a prime element] if and only if ue is an atom [a prime element].*
2. *Every prime element of D is an atom.*
3. *D is factorial if and only if D is atomic and every atom of D is a prime element.*
4. (Uniqueness of prime factorizations) *Suppose that $k, l \in \mathbb{N}_0$, $e \in D^\times$, let $p_1, \ldots, p_k, q_1, \ldots, q_l \in D^\bullet$ be prime elements and $p_1 \cdot \ldots \cdot p_k = eq_1 \cdot \ldots \cdot q_l$. Then $k = l$, and there is a permutation $\pi \in \mathfrak{S}_k$ such that, for all $i \in [1, k]$, $p_i = q_{\pi(i)} e_i$ for some $e_i \in D^\times$.*

PROOF. 1. If $a = be$ for some $e \in D^\times$, then clearly $aD = bD$. Thus assume that $aD = bD$. If $a = 0$, then $b = 0$ and there is nothing to do. If $a \neq 0$, then $b \neq 0$, and since $a \in bD$ and $b \in aD$, there exist elements $c, d \in D$ such that $a = bc$ and $b = ad$. Consequently, $a = adc$, hence $dc = 1$ and $c \in D^\times$.

If $u \in D$ and $e \in D^\times$, then $uD = ueD$. As atoms and prime elements are characterized by properties of the principal ideals which they generate, it follows that u is an atom [a prime element] if and only if the same holds for ue.

2. Let p be a prime element, and suppose that $p = ab$, where $a, b \in D$. Since $ab \in pD$, it follows that $a \in pD$ or $b \in pD$, and we may assume that $a \in pD$. Since $p \in aD$, we obtain $abD = pD = aD$ and therefore $b \in D^\times$.

3. If D is atomic and every atom is a prime element, then D is factorial by definition. Thus suppose that D is factorial. Then D is atomic, since every prime element is an atom. If $u \in D$ is an atom, then $u = ep_1 \cdot \ldots \cdot p_k$, where $k \in \mathbb{N}_0$, $e \in D^\times$, and $p_1, \ldots, p_k$ are prime elements. Since u is irreducible, we obtain $k = 1$, and therefore $u = ep_1$ is a prime element.

4. We use induction on k. If $k = 0$, then $l = 0$, and there is nothing to do.

$k \geq 1$, $k-1 \to k$: Since $p_1 \cdot \ldots \cdot p_k \notin D^\times$, we have $l \geq 1$, and since $p_1 \cdot \ldots \cdot p_k \in q_l D$, there is some $i \in [1, k]$ such that $p_i \in q_l D$, hence $p_i D \subset q_l D \subsetneq D$. But p_i is an atom, and therefore $p_i D = q_l D$ and $p_i = q_l v$ for some $v \in D^\times$. After renumbering if necessary, we may assume that $i = k$. Then $p_1 \cdot \ldots \cdot p_{k-1} = evq_1 \cdot \ldots \cdot q_{l-1}$, $ev \in D^\times$, and the assertion follows by the induction hypothesis. $\square$

The definition of greatest common divisors in general integral domains charges some care. Suppose that $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in D$.

- An element $d \in D$ is called a *greatest common divisor* of $a_1, \ldots, a_n$ if dD is the smallest principal ideal of D containing $\{a_1, \ldots, a_n\}$.
- $a_1, \ldots, a_n$ are called *coprime* if the principal ideals $a_1D, \ldots, a_nD$ are coprime [that means, $a_1D + \ldots + a_nD = D$]. By definition, $a_1, \ldots, a_n$ are coprime if and only if there exist $x_1, \ldots, x_n \in D$ such that $a_1x_1 + \ldots + a_nx_n = 1$. In this case, we write $(a_1, \ldots, a_n) = 1$. If $a, b \in D$ and $(a, b) = 1$, then we say also that a and b are coprime or that a is coprime to b.

Note that $a_1, \ldots, a_n$ need not have a greatest common divisor, but if d is a greatest common divisor of $a_1, \ldots, a_n$, then $dD^\times$ is the set of all greatest common divisors of $a_1, \ldots, a_n$. If $a_1, \ldots, a_n$ are coprime, then 1 is a greatest common divisor of $a_1, \ldots, a_n$, but the converse need not be true (in $\mathbb{Z}[X, Y]$ the elements X and Y are not coprime, but 1 is a greatest common divisor of X and Y).

For $D = \mathbb{Z}$, the above definitions coincide with those from Section A.3. The theory of coprime elements carries over to general integral domains without any problems (see Theorem A.8.2), but the theory of the greatest common divisors in general integral domains is a subject of algebraic number theory and multiplicative ideal theory. We refer to [**24**]. Here we present the theory of greatest common divisors for principal ideal domains which is sufficient for the purposes of this volume (see Theorem A.8.3).

Recall that, for any integral domain D and $a, b, d \in D$, we write $a \equiv b \mod d$ instead of $a \equiv b \mod dD$ [or $a - b \in dD$].

Theorem A.8.2. *Suppose that* $a, b, c, x, y \in D$.

1. *If* $(a, b) = 1$ *and* $(a, c) = 1$, *then* $(a, bc) = 1$ *and* $(a, b+da) = 1$ *for all* $d \in D$. *More generally, if* $m, n \in \mathbb{N}$ *and* $a_1, \ldots, a_n, b_1, \ldots, b_m \in D$ *are such that* $(a_i, b_j) = 1$ *for all* $i \in [1, n]$ *and* $j \in [1, m]$, *then* $(a_1 \cdot \ldots \cdot a_n, b_1 \cdot \ldots \cdot b_m) = 1$.
2. *If* $bc \in aD$ *and* $(a, b) = 1$, *then* $c \in aD$.
3. *If* $ax \equiv ay \mod b$ *and* $(a, b) = 1$, *then* $x \equiv y \mod b$.
4. *If* $x \equiv y \mod b$ *and* $(x, b) = 1$, *then* $(y, b) = 1$.
5. *If* $\mathbb{Z} \subset D$ *and* p *is a prime, then* $(x + y)^p \equiv x^p + y^p \mod p$.

Proof. 1. Let $s, t, u, v \in D$ be such that $as + bt = au + cv = 1$. Then it follows that $1 = (as + bt)(au + cv) = a(sau + scv + btu) + bc(tv)$, and therefore $(a, bc) = 1$. If $d \in D$, then $a(s - dt) + (b + da)t = 1$, and thus $(a, b + da) = 1$. The more general assertion follows by an obvious double induction on m and n.

2. Let $s, t, u \in D$ be such that $bc = au$ and $as + bt = 1$. Then it follows that $c = cas + cbt = a(cs + ut) \in aD$.

3. If $ax - ay = a(x - y) \in bD$ and $(a, b) = 1$, then $x - y \in bD$ by 3.

4. Let $u, s, t \in D$ be such that $x - y = bu$ and $xs + bt = 1$. Then it follows that $1 = (y + bu)s + bt = ys + b(us + t)$, and therefore $(y, b) = 1$.

5. If p is a prime, then

$$\binom{p}{i} \in p\mathbb{Z} \subset pD \quad \text{for all } \ i \in [1, p-1]\,,$$

and therefore

$$(x+y)^p - x^p - y^p = \sum_{i=1}^{p-1} \binom{p}{i} x^i y^{p-i} \in pD\,. \qquad \square$$

Theorem A.8.3. *Let D be a principal ideal domain and $K = \mathsf{q}(D)$.*

1. *D is factorial, and every non-zero prime ideal of D is a maximal ideal.*
2. *If $n \in \mathbb{N}$ and $a_1, \ldots, a_n$, $d \in D$, then the following assertions are equivalent:*
   - (a) *d is a greatest common divisor of $a_1, \ldots, a_n$.*
   - (b) *$a_1D + \ldots + a_nD = dD$.*
   - (c) *$\{a_1, \ldots, a_n\} \subset dD$, and if $d \neq 0$, then $(d^{-1}a_1, \ldots, d^{-1}a_n) = 1$.*

   In particular, $a_1, \ldots, a_n$ have a greatest common divisor, and $a_1, \ldots, a_n$ are coprime if and only if 1 is a greatest common divisor of $a_1, \ldots, a_n$.
3. *Suppose that $a \in D$ and $b = p_1 \cdot \ldots \cdot p_n$, where $k \in \mathbb{N}$ and $p_1, \ldots, p_n$ are prime elements of D. Then $(a, p) = 1$ if and only if $a \notin p_iD$ for all $i \in [1, n]$. In particular, if p is a prime element of D, then $(a, p) = 1$ if and only if $a \in D \setminus pD$.*
4. *If $K = \mathsf{q}(D)$, then every $x \in K$ is of the form $x = a^{-1}b$, where $b \in D$, $a \in D^\bullet$, and $(a, b) = 1$. In this representation, the ideals aD and bD are uniquely determined by x.*

Proof. 1. Let S be the set of all $a \in D^\bullet \setminus D^\times$ which cannot be written as a product of prime elements. If $a \in S$, then a is not an atom, hence there is a factorization $a = a'a''$, where a', $a'' \in D^\bullet \setminus D^\times$, hence $aD \subsetneq a'D$, $aD \subsetneq a''D$, and either a' or a'' belongs to S. For every $a \in S$ we fix an element $a' \in S$ such that $aD \subsetneq a'D$.

Assume now that $S \neq \emptyset$, fix an element $a \in S$ and define the sequence $(a_i)_{i \geq 0}$ in S recursively by $a_0 = a$ and $a_{i+1} = a_i'$ for all $i \geq 0$. It follows that $a_iD \subsetneq a_{i+1}D$ for all $i \geq 0$, and

$$J = \bigcup_{i \geq 0} a_iD$$

is an ideal of D, say $J = bD$ for some $b \in D$. Then there is some $n \geq 0$ such that $b \in a_nD$, which implies $bD = a_iD$ for all $i \geq n$, a contradiction.

If $\mathfrak{p} \subset D$ is a non-zero prime ideal, then $\mathfrak{p} = pD$ for some prime element $p \in D$. Since p is an atom, the ideal pD is maximal among proper principal ideals, and therefore it is a maximal ideal.

2. (a) $\Leftrightarrow$ (b) By definition, d is a greatest common divisor of $a_1, \ldots, a_n$ if and only if dD is the smallest principal ideal containing $\{a_1, \ldots, a_n\}$. On the other hand, $a_1D + \ldots + a_nD$ is the smallest ideal containing $\{a_1, \ldots, a_n\}$, and it is a principal ideal. Hence d is a greatest common divisor of $a_1, \ldots, a_n$ if and only if $dD = a_1D + \ldots + a_nD$.

(b) $\Rightarrow$ (c) By definition, $\{a_1,\ldots,a_n\} \subset a_1D+\ldots+a_nD = dD$, and if $d \neq 0$, then $d^{-1}a_1D+\ldots+d^{-1}a_nD = D$, and therefore $(d^{-1}a_1,\ldots,d^{-1}a_n)=1$.

(c) $\Rightarrow$ (b) If $d=0$, there is nothing to do. If $d \neq 0$, then $(d^{-1}a_1,\ldots,d^{-1}a_n)=1$ implies $d^{-1}a_1D+\ldots+d^{-1}a_nD = D$, and therefore $a_1D+\ldots+a_nD=D$.

Since every ideal is principal, (b) implies that $a_1,\ldots,a_n$ have a greatest common divisor, and the equivalence of (a) and (b), applied with $d=1$, shows that $a_1,\ldots,a_n$ are coprime if and only if 1 is a greatest common divisor of $a_1,\ldots,a_n$.

3. If $a \in p_iD$ for some $i \in [1,n]$, then $(a,b) \neq 1$. Conversely, assume that $a \notin p_iD$ for all $i \in [1,n]$. By 1., p_iD is a maximal ideal of D, hence $aD+p_iD=D$, and there exist elements u_i, $v_i \in D$ such that $1 = au_i+p_iv_i$. It follows that

$$1 = \prod_{i=1}^{n}(au_i+p_iv_i) = au + p_1\cdot\ldots\cdot p_nv = au+bv$$

for some $u \in D$ and $v = v_1\cdot\ldots\cdot v_n$. Hence it follows that $(a,b)=1$.

4. Suppose that $x = a_0^{-1}b_0 \in K$, where $a_0 \in D^\bullet$ and $b_0 \in D$. If $d \in D^\bullet$ is a greatest common divisor of a_0 and b_0, $a = d^{-1}a_0$ and $b = d^{-1}b_0$, then $(a,b)=1$ and $x = a^{-1}b$. To prove uniqueness, assume that $x = a^{-1}b = a_1^{-1}b_1$, where a, $a_1 \in D^\bullet$, b, $b_1 \in D$, $(a,b)=1$ and $(a_1,b_1)=1$. Then $a_1b = ab_1 \in aD$, and thus $a_1 \in aD$ by Theorem A.8.2.2. By symmetry it follows that $a \in a_1D$, hence $aD = a_1D$, and finally $bD = b_1D$, since $aa_1 \neq 0$. □

We close this section with a characterization of the unit group of a residue class ring. As a consequence, we can extend the notion of congruences in general integral domains to fractions with a denominator coprime to the modulus.

Lemma A.8.4. *Let $\mathfrak{a}$ be an ideal of D and $c \in D$. Then $c+\mathfrak{a} \in (D/\mathfrak{a})^\times$ if and only if $\mathfrak{a}+cD=D$. In particular, if $a \in D$, then $c+aD \in (D/aD)^\times$ if and only if $(c,a)=1$.*

Proof. If $c+\mathfrak{a} \in (D/\mathfrak{a})^\times$, then $cd+\mathfrak{a} = (c+\mathfrak{a})(d+\mathfrak{a}) = 1+\mathfrak{a}$ for some $d \in D$. Hence $1 \in \mathfrak{a}+cd \subset \mathfrak{a}+cD$, and therefore $\mathfrak{a}+cD=D$.

Conversely, if $\mathfrak{a}+cD=D$, then there exist elements $a \in \mathfrak{a}$ and $d \in D$ such that $1 = a+cd$, and then $(c+\mathfrak{a})(d+\mathfrak{a}) = cd+\mathfrak{a} = 1+\mathfrak{a}$, which shows that $c+\mathfrak{a} \in (D/\mathfrak{a})^\times$. □

Now we define fractions with coprime denominators. Let K be a quotient field of D and $b \in D$. Then we define

$$D_{[b]} = \{a^{-1}c \mid c \in D\,,\ a \in D^\bullet,\ (a,b)=1\,\} \subset K\,.$$

If b, $b_1 \in D$ and $b_1D \subset bD$, then it follows (using Theorem A.8.2) that

$$D = D_{[0]} \subset D_{[b_1]} \subset D_{[b]} \subset D_{[1]} = K\,.$$

Theorem and Definition A.8.5. *Let K be a quotient field of D and $b \in D$.*

1. *$D_{[b]}$ is a subring of K, and $D_{[b]}^\times = \{a^{-1}c \mid a,\, c \in D^\bullet,\ (a,b) = (c,b) = 1\}$.*
2. *$bD_{[b]} \cap D = bD$, and there is an isomorphism*

$$\Phi\colon D/bD \xrightarrow{\sim} D_{[b]}/bD_{[b]}\,, \quad \text{given by} \quad \Phi(c+bD) = c + bD_{[b]} \quad \text{for all } c \in D.$$

We identify the residue class rings D/bD and $D_{[b]}/bD_{[b]}$ by means of Φ. For $x,\, y \in D_{[b]}$, we set $x \equiv y \bmod b$ (in D) if and only if $x - y \in bD_{[b]}$.

If $x = a^{-1}c \in D_{[b]}$, where $c \in D$, $a \in D^\bullet$ and $(a,b) = 1$, then we have $a + bD \in (D/bD)^\times$, and

$$x + bD_{[b]} = (a+bD)^{-1}(c+bD) \in D/bD = D_{[b]}/bD_{[b]}\,.$$

Proof. 1. Suppose that $x,\, x_1 \in D_{[b]}$, say $x = a^{-1}c$ and $x_1 = a_1^{-1}c_1$, where $c,\, c_1 \in D$, $a,\, a_1 \in D^\bullet$ and $(a,b) = (a_1,b) = 1$. Then it follows that $(aa_1,b) = 1$, hence $x - y = (aa_1)^{-1}(a_1c - ac_1) \in D_{[b]}$ and $xy = (aa_1)^{-1}(cc_1) \in D_{[b]}$. Therefore $D_{[b]}$ is a subring of K.

If $x = a^{-1}c$, where $a,\, c \in D^\bullet$ and $(a,b) = (c,b) = 1$, then $x^{-1} = c^{-1}a$, hence $x,\, x^{-1} \in D_{[b]}$ and $x \in D_{[b]}^\times$. Conversely, assume that $x = a^{-1}c \in D_{[b]}^\times$, where $c \in D$, $a \in D^\bullet$ and $(a,b) = 1$. Then $x^{-1} \in D_{[b]}$, say $x^{-1} = a_1^{-1}c_1$, where $c_1 \in D$, $a_1 \in D^\bullet$ and $(a_1,b) = 1$. We obtain $1 = xx^{-1} = (aa_1)^{-1}cc_1$, hence $cc_1 = aa_1$, and since $(cc_1,b) = (aa_1,b) = 1$, we obtain $(c,b) = 1$.

2. Obviously, $bD \subset bD_{[b]} \cap D$. Thus suppose that $x \in bD_{[b]} \cap D$, say $x = ba^{-1}c$, where $c \in D$, $a \in D^\bullet$ and $(a,b) = 1$. Then $ax = bc \in bD$, and $(a,b) = 1$ implies $x \in bD$ by Theorem A.8.2.2.

The map $\Phi_0\colon D \to D_{[b]}/bD_{[b]}$, defined by $\Phi_0(x) = x + bD_{[b]}$, is a ring homomorphism with kernel $bD_{[b]} \cap D = bD$, and we assert that Φ_0 is surjective. Once this is proved, it follows that Φ_0 induces an isomorphism Φ as asserted.

Suppose that $x = a^{-1}c \in D_{[b]}$, where $c \in D$, $a \in D^\bullet$, $(a,b) = 1$, and let $u,\, v \in D$ be such that $au + bv = 1$. Then $x = a^{-1}c(au+bv) = cu + a^{-1}bv$, and $x + bD_{[b]} = cu + bD_{[b]} = \Phi_0(cu + bD)$.

To prove the final assertion, assume that $x = a^{-1}b$, where $c \in D$, $a \in D^\bullet$ and $(a,b) = 1$. Then Lemma A.8.4 implies $a + bD \in (D/bD)^\times = (D_{[b]}/bD_{[b]})^\times$. Thus we get $(x + bD_{[b]})(a + bD_{[b]}) = ax + bD_{[b]} = c + bD_{[b]}$, and therefore

$$x + bD_{[b]} = (a + bD_{[b]})^{-1}(c + bD_{[b]}) = (a+bD)^{-1}(c+bD)\,. \qquad \square$$

A.9. Algebraic integers

A thorough theory of algebraic integers is the topic of algebraic number theory, and we refer the reader to corresponding textbooks such as [**83**] or [**85**]. Here we limit ourselves to some elementary facts which are used in some arguments given in the Chapters 3, 5 and 7. In particular, we introduce the notion of an algebraic integer, we investigate how to handle congruences between them, and we study some properties of coprime algebraic integers.

For $k \in \mathbb{N}$ and $z_1, \ldots, z_k \in \mathbb{C}$, we denote by $\mathbb{Z}[z_1, \ldots, z_k]$ the smallest subring of $\mathbb{C}$ containing $z_1, \ldots, z_k$ and call it the *number ring generated by* $z_1, \ldots, z_k$. Explicitly, $\mathbb{Z}[z_1, \ldots, z_k]$ consists of all numbers of the form

$$\sum_{i_1=0}^{N} \cdots \sum_{i_k=0}^{N} c_{i_1,\ldots,i_k} z_1^{i_1} \cdot \ldots \cdot z_k^{i_k}\,, \quad \text{where} \quad N \in \mathbb{N} \quad \text{and} \quad c_{i_1,\ldots,i_k} \in \mathbb{Z} \quad \text{for all} \quad (i_1, \ldots, i_k)\,.$$

For $k = 0$, we understand that $\mathbb{Z}[z_1, \ldots, z_k] = \mathbb{Z}$. If $k \geq 2$, then $\mathbb{Z}[z_1, \ldots, z_k]$ consists of all numbers of the form

$$\sum_{i=0}^{N} b_i z_k^i\,, \quad \text{where} \quad N \in \mathbb{N} \quad \text{and} \quad b_i \in \mathbb{Z}[z_1, \ldots, z_{k-1}] \quad \text{for all } i \in [0, N]\,,$$

and if $z \in \mathbb{C}$, then $\mathbb{Z}[z] = \{c_0 + c_1 z + \ldots + c_N z^N \mid N \in \mathbb{N}_0\,,\ c_1, \ldots, c_N \in \mathbb{Z}\,\}$.

A complex number z is called

- *algebraic* if $z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0 = 0$ for some $n \in \mathbb{N}$ and $a_0, \ldots, a_{n-1} \in \mathbb{Q}$ (such an equation is called an *algebraic equation* for z);
- an *algebraic integer* if $z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0 = 0$ for some $n \in \mathbb{N}$ and $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ (such an equation is called an *integral equation* for z).

We denote by

- $\overline{\mathbb{Q}}$ the set of all algebraic numbers, and by
- $\overline{\mathbb{Z}}$ the set of all algebraic integers.

Obviously, $\mathbb{Z} \subset \overline{\mathbb{Z}}$, $\mathbb{Q} \subset \overline{\mathbb{Q}}$, $\overline{\mathbb{Z}} \subset \overline{\mathbb{Q}}$, and every root of unity is an algebraic integer. In Corollary A.9.4 we shall see that $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$ (a rational algebraic integer is an integer).

Theorem A.9.1.

1. *If* $k \in \mathbb{N}_0$ *and* $z_1, \ldots, z_k \in \overline{\mathbb{Z}}$, *then* $\mathbb{Z}[z_1, \ldots, z_k] \subset \overline{\mathbb{Z}}$, *and* $\mathbb{Z}[z_1, \ldots z_k]$ *is a finitely generated* (*additive*) *abelian group.*
2. $\overline{\mathbb{Z}}$ *is a subring of* $\mathbb{C}$, *and* $\overline{\mathbb{Q}} = \{z \in \mathbb{C} \mid mz \in \overline{\mathbb{Z}} \text{ for some } m \in \mathbb{N}\,\} = \mathsf{q}(\overline{\mathbb{Z}})$.

Proof. 1. We first use induction on k to prove that $\mathbb{Z}[z_1, \ldots, z_k]$ is finitely generated. For $k = 0$ there is nothing to do.

$k \geq 1\,,\ k-1 \to k$: By the induction hypothesis, there exist some $m \in \mathbb{N}_0$ and $u_1, \ldots, u_m \in \mathbb{C}$ such that $D = \mathbb{Z}[z_1, \ldots, z_{k-1}] = \mathbb{Z}u_1 + \ldots + \mathbb{Z}u_m$, and we set $z = z_k$. Let $n \in \mathbb{N}$ and $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ be such that $z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0 = 0$ is an integral equation for z. Then

$$M = \sum_{j=1}^{m} \sum_{i=0}^{n-1} \mathbb{Z} u_j z^i = \sum_{i=0}^{n-1} D z^i \subset \mathbb{Z}[z_1, \ldots, z_k]$$

is a finitely generate subgroup, and we shall prove that $M = \mathbb{Z}[z_1, \ldots, z_k]$. Since every $x \in \mathbb{Z}[z_1, \ldots, z_k]$ is of the form $x = c_0 + c_1 z + \ldots + c_N z^N$, where $N \in \mathbb{N}_0$ and $c_0, \ldots, c_N \in D$, it suffices to prove that $z^\nu \in M$ for all $\nu \in \mathbb{N}_0$. We do this by induction on ν. For $\nu < n$, there is nothing to do. Thus assume that $\nu > n$ and $z^i \in M$ for all $i \in [0, \nu-1]$. Then we obtain (using the integral equation for z)

$$z^\nu = z^{\nu-n} z^n = z^{\nu-n}\Big(-\sum_{i=0}^{n-1} a_i z^i\Big) = \sum_{i=0}^{n-1} (-a_i) z^{i+\nu-n} \in M\,.$$

Now we can prove that $\mathbb{Z}[z_1, \ldots, z_k] \subset \overline{\mathbb{Z}}$. As $\mathbb{Z}[z_1, \ldots, z_k]$ is a finitely generated group, there exist some $m \in \mathbb{N}$ and $u_1, \ldots, u_m \in \mathbb{Z}[z_1, \ldots, z_k]^\bullet$ such that $\mathbb{Z}[z_1, \ldots, z_k] = \mathbb{Z}u_1 + \ldots + \mathbb{Z}u_m$. If $x \in \mathbb{Z}[z_1, \ldots, z_k]$, then $xu_j \in \mathbb{Z}u_1 + \ldots + \mathbb{Z}u_m$ for all $j \in [1, m]$, and thus there exists a matrix $A = (a_{i,j})_{i,\, j \in [1,m]} \in \mathsf{M}_m(\mathbb{Z})$ such that

$$xu_j = \sum_{i=0}^{m} a_{i,j} u_i \quad \text{for all} \quad j \in [0, m]\,, \text{ and therefore } (u_1, \ldots, u_m)(xI - A) = \mathbf{0}\,.$$

As $(u_1, \ldots, u_m) \neq \mathbf{0}$, it follows from the theory of linear homogeneous equations that $\det(xI - A) = 0$. We expand this determinant and obtain an equation

$$x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0 = 0 \quad \text{for some} \quad a_0, \ldots, a_{m-1} \in \mathbb{Z}\,.$$

Hence x is an algebraic integer.

2. If $x,\ y \in \overline{\mathbb{Z}}$, then $\{x - y,\ xy\} \subset \mathbb{Z}[x, y] \subset \overline{\mathbb{Z}}$, and therefore $\overline{\mathbb{Z}}$ is a subring of $\mathbb{C}$.

We prove next that $\overline{\mathbb{Q}} = \{z \in \mathbb{C} \mid mz \in \overline{\mathbb{Z}} \text{ for some } m \in \mathbb{N}\}$. If $z \in \overline{\mathbb{Q}}$, then z satisfies an algebraic equation $z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0 = 0$ for some $n \in \mathbb{N}$ and $a_0, \ldots, a_{n-1} \in \mathbb{Q}$. If $m \in \mathbb{N}$ is such that $ma_i \in \mathbb{Z}$ for all $i \in [0, n-1]$, then $(mz)^n + ma_{n-1}(mz)^{n-1} + \ldots + m^{n-1}a_1(mz) + m^n a_0 = 0$ is an integral equation for mz, and thus $mz \in \overline{\mathbb{Z}}$. Conversely, if $z \in \mathbb{C}$, $m \in \mathbb{N}$ and $mz \in \overline{\mathbb{Z}}$, then there exists an integral equation for mz, say $(mz)^n + a_{n-1}(mz)^{n-1} + \ldots + a_1(mz) + a_0 = 0$, where $n \in \mathbb{N}$ and $a_0, \ldots, a_{n-1} \in \mathbb{Z}$. Dividing this equation by m^n, we obtain an algebraic equation for z, which shows that $z \in \overline{\mathbb{Q}}$.

In order to prove that $\overline{\mathbb{Q}}$ is a quotient field of $\overline{\mathbb{Z}}$, it is now sufficient to show that $\overline{\mathbb{Q}}$ is a field. If $z_1,\ z_2 \in \overline{\mathbb{Q}}$, then there exist $m_1,\ m_2 \in \mathbb{N}$ such that $\{m_1 z_1, m_2 z_2\} \subset \overline{\mathbb{Z}}$. Then $m_1 m_2(z_1 - z_2) \in \overline{\mathbb{Z}}$ and $m_1 m_2 z_1 z_2 \in \overline{\mathbb{Z}}$, hence $\{z_1 - z_2, z_1 z_2\} \subset \overline{\mathbb{Q}}$, and therefore $\overline{\mathbb{Q}}$ is a subring of $\mathbb{C}$. For $z \in \overline{\mathbb{Q}}^\bullet$, let $n \in \mathbb{N}$ be minimal such that there exist $a_0, \ldots, a_{n-1} \in \mathbb{Q}$ satisfying $z^n + a_{n-1}z^{n-1} + \ldots + a_1 z + a_0 = 0$. Then $a_0 \neq 0$, and the equation $(z^{-1})^n + a_0^{-1}a_1(z^{-1})^{n-1} + \ldots + a_0^{-1}a_{n-1}\, z^{-1} + a_0^{-1} = 0$ shows that $z^{-1} \in \overline{\mathbb{Q}}$. $\square$

For the ring $\overline{\mathbb{Z}}$ of algebraic integers, we use the notions of coprime elements and (fractional) congruences as we did in Section A.8 for arbitrary integral domains. However, we have to be careful when we want to apply the notions for subrings of $\overline{\mathbb{Z}}$ instead for $\overline{\mathbb{Z}}$ itself. This causes no problems for coprime elements (see Theorem A.9.2), but needs additional assumptions for congruences (see Theorem A.9.3).

Theorem A.9.2. *Let D be a subring of $\overline{\mathbb{Z}}$, $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in D$. Then*

$$a_1\overline{\mathbb{Z}} + \ldots + a_n\overline{\mathbb{Z}} = \overline{\mathbb{Z}} \quad \textit{if and only if} \quad a_1 D + \ldots + a_n D = D\,.$$

In particular, the relation $(a_1, \ldots, a_n) = 1$ holds regardless of the domain in which it is considered.

Proof. Obviously, $a_1D + \ldots + a_nD = D$ implies $a_1\overline{\mathbb{Z}} + \ldots + a_n\overline{\mathbb{Z}} = \overline{\mathbb{Z}}$. For the converse, assume that $a_1\overline{\mathbb{Z}} + \ldots + a_n\overline{\mathbb{Z}} = \overline{\mathbb{Z}}$, hence $1 = a_1x_1 + \ldots + a_nx_n$ for some $a_1, \ldots, a_n \in \overline{\mathbb{Z}}$. We consider the ideal $\mathfrak{a} = a_1D + \ldots + a_nD$ of D, and we must prove that $1 \in \mathfrak{a}$. By Theorem A.9.1.1 we obtain $\mathbb{Z}[x_1, \ldots, x_n] = \mathbb{Z}u_1 + \ldots + \mathbb{Z}u_m$ for some $m \in \mathbb{N}$ and $u_1, \ldots, u_m \in \mathbb{Z}[x_1, \ldots, x_n]^\bullet \subset \overline{\mathbb{Z}}$. Hence, for $\nu \in [1, n]$ and $\mu, i, j \in [1, m]$, there exist $b_{\nu,\mu}$, $c_{\mu,i,j} \in \mathbb{Z}$ such that

$$x_\nu = \sum_{\mu=1}^{m} b_{\nu,\mu}u_\mu \quad \text{and} \quad u_\mu u_i = \sum_{j=1}^{m} c_{\mu,i,j}u_j \quad \text{for all } \nu \in [1, n] \text{ and } \mu, i \in [1, m].$$

Therefore we obtain, for all $i \in [1, m]$,

$$u_i = \sum_{\nu=1}^{n} a_\nu x_\nu u_i = \sum_{\nu=1}^{n} a_\nu \sum_{\mu=1}^{m} b_{\nu,\mu}u_\mu u_i = \sum_{\nu=1}^{n} a_\nu \sum_{\mu=1}^{m} b_{\nu,\mu} \sum_{j=1}^{m} c_{\mu,i,j}u_j = \sum_{j=1}^{m} d_{i,j}u_j\,,$$

where

$$d_{i,j} = \sum_{\nu=1}^{n}\sum_{\mu=1}^{m} a_\nu b_{\nu,\mu}c_{\mu,i,j} \in \mathfrak{a} \quad \text{for all } \ i,\, j \in [1, m]\,.$$

In particular, it follows that

$$\sum_{j=1}^{m}(\delta_{i,j} - d_{i,j})u_j = 0 \quad \text{for all } \ i \in [1, m]\,.$$

By the theory of linear homogeneous equations we get $\det(\delta_{i,j} - d_{i,j})_{i,j\in[1,m]} = 0$, and expanding this determinant gives an equation showing that $0 \in 1 + \mathfrak{a}$, and consequently $1 \in \mathfrak{a}$. □

A subring D of $\overline{\mathbb{Z}}$ is called *integrally closed* if $D = \overline{\mathbb{Z}} \cap \mathsf{q}(D)$.

Theorem A.9.3. *Le D be a subring of $\overline{\mathbb{Z}}$.*

1. *If D is a principal ideal domain, then D is integrally closed.*
2. *Let D be integrally closed and $d \in D$. Then $d\overline{\mathbb{Z}} \cap D = dD$, and if $x, y \in D$, then the congruence $x \equiv y \bmod d$ holds in $\overline{\mathbb{Z}}$ if and only if it holds in D.*

Proof. 1. If $K = \mathsf{q}(D)$, then it is obvious that $D \subset \overline{\mathbb{Z}} \cap K$. Thus assume that D is a principal ideal domain and $x \in K \cap \overline{\mathbb{Z}}$. By Theorem A.8.3.3, $x = a^{-1}b$, where $a \in D^\bullet$, $b \in D$ and $(a, b) = 1$. Let $n \in \mathbb{N}$ and $a_0, \ldots, a_{n-1} \in \mathbb{Z}$ be such that $x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0$ is an integral equation for x. Then we obtain

$$\begin{aligned} 0 &= a^n(x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0) \\ &= b^n + a_{n-1}ab^{n-1} + \ldots + a_1a^{n-1}b + a_0a^n = b^n + ac \quad \text{for some } c \in D. \end{aligned}$$

Since $(a, b) = 1$, it follows that $(a, b^n) = 1$, and there exist $u, v \in D$ such that $1 = au + b^nv = a(u - c)$. Hence $a \in D^\times$ and $x \in D$.

2. Obviously, $dD \subset d\overline{\mathbb{Z}} \cap D$. Thus suppose that $x = dz \in d\overline{\mathbb{Z}} \cap D$, where $z \in \overline{\mathbb{Z}}$. Then it follows that $z = d^{-1}x \in \overline{\mathbb{Z}} \cap K = D$ and thus $x \in dD$. □

Corollary A.9.4. $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$. *In particular, if* $a, b \in \mathbb{Z}$ *and* $m \in \mathbb{N}$, *then the congruence* $a \equiv b \bmod m$ *holds in* $\overline{\mathbb{Z}}$ *if and only if it holds in* $\mathbb{Z}$.

Proof. By Theorem A.9.3. □

APPENDIX B

Some results from analysis

In this section, we gather some results from analysis which we used in the Chapters 4 and 8. As we assume that the reader is familiar with standard real analysis, we confine ourselves to some additional topics. In Section B.1 we give an overview of some basis results from complex analysis without proofs, and in Section B.2 we present some probably less known results from real analysis, this time with detailed proofs.

For more details and proofs, the reader should consult any substantial textbook on analysis such as the classical books [**109**] or [**3**].

B.1. Notational conventions and results from complex analysis

For a real number ϑ, we denote the open and the closed right half-plane determined by ϑ by

$$\mathcal{H}_\vartheta = \{s \in \mathbb{C} \mid \Re(s) > \vartheta\} \quad \text{and} \quad \overline{\mathcal{H}}_\vartheta = \{s \in \mathbb{C} \mid \Re(s) \ge \vartheta\}\,.$$

For x, $X \in \mathbb{R}$ and $m \in \mathbb{N}$, we write

$$\sum_{n<x}, \quad \sum_{x \le n < X}, \quad \sum_{n>X}, \quad \sum_{n \,|\, m} \quad \text{etc.} \quad \text{resp.} \quad \sum_{p<x}, \quad \sum_{x \le p < X}, \quad \sum_{p>X}, \quad \sum_{p \,|\, m} \quad \text{etc.}$$

to denote the (eventually infinite) sum over all $n \in \mathbb{N}$ resp. all primes p satisfying the corresponding conditions.

Results from complex analysis. Let $\emptyset \ne D \subset \mathbb{C}$ be an open subset.

1. A function $f\colon D \to \mathbb{C}$ is called *holomorphic* or *analytic* if it is (complex) differentiable in D. If this is the case, then

- f is infinitely differentiable in D;
- If $s_0 \in D$, $r \in \mathbb{R}_{>0}$ and $B(r, s_0) = \{s \in \mathbb{C} \mid |s - s_0| \le r\} \subset D$, then

$$f(s) = \sum_{k=0}^{\infty} \frac{f^{(k)}(s_0)}{k!}(s - s_0)^k \quad \text{for all} \quad s \in B_(r, s_0)\,.$$

2. Suppose that $s_0 \in D$ and $(a_n)_{n \ge 0}$ is a sequence of complex numbers such that the power series

$$f(s) = \sum_{n=0}^{\infty} a_n (s - s_0)^n$$

converges for all $s \in D$. Then this power series converges absolutely and uniformly in each compact subset of D and defines a holomorphic function $f\colon D \to \mathbb{C}$. For all $s \in D$ and $k \in \mathbb{N}_0$ we have

$$f^{(k)}(s) = \sum_{n=k}^{\infty} n(n-1) \cdot \ldots \cdot (n-k+1)(s-s_0)^{n-k}\,.$$

3. The exponential series

$$\exp(z) = \sum_{n=0}^{\infty} \frac{z^n}{n!}$$

defines a holomorphic function $\exp\colon \mathbb{C} \to \mathbb{C}$ such that

- $\exp(\mathbb{C}) = \mathbb{C}^{\times}$,
- $\exp(z_1 + z_2) = \exp(z_1)\exp(z_2)$ for all $z_1,\, z_2 \in \mathbb{C}$,
- $|\exp(z)| = 1$ if and only if $z \in 2\pi \mathrm{i}\mathbb{Z}$,

and

$$\frac{1}{1-z} = \exp\Bigl(\sum_{j=1}^{\infty} \frac{z^j}{j}\Bigr) \quad \text{for all} \quad z \in \mathbb{C} \quad \text{such that} \quad |z| < 1\,.$$

For $s \in \mathbb{C}$ and $a \in \mathbb{R}_{>0}$, we set ${}^{a}\exp(s) = a^s = \exp(s \log a)$. Then ${}^{a}\exp\colon \mathbb{C} \to \mathbb{C}$ is a holomorphic function, $\mathrm{e}^s = \exp(s)$, and if $z = x + \mathrm{i}y$ for some $x,\, y \in \mathbb{R}$, then $\exp(z) = \mathrm{e}^x(\cos y + \mathrm{i}\sin(y))$ and $|\exp(z)| = \mathrm{e}^x$.

4. (Weierstrass criterion for series) Let $(f_n\colon D \to \mathbb{C})_{n\geq 0}$ be a sequence of holomorphic functions. Suppose that for each compact subset K of D there is a sequence $(A_n)_{n\geq 0}$ in $\mathbb{R}_{\geq 0}$ such that

$$|f_n(s)| \leq A_n \quad \text{for all} \quad s \in K\,, \qquad \text{and} \qquad \sum_{n=0}^{\infty} A_n < \infty\,.$$

Then the series

$$F(s) = \sum_{n=0}^{\infty} f_n(s)$$

converges (absolutely and uniformly) for all $s \in D$ and defines a holomorphic function $F\colon D \to \mathbb{C}$. For all $s \in D$ and $k \in \mathbb{N}_0$ we have

$$F^{(k)}(s) = \sum_{n=0}^{\infty} f_n^{(k)}(s)\,.$$

5. (Weierstrass criterion for integrals) Let $f\colon D \times \mathbb{R}_{\geq 1} \to \mathbb{C}$ be a function with the following properties:

- $f(\,\cdot\,, \xi)\colon D \to \mathbb{C}$ is holomorphic for every $\xi \in \mathbb{R}_{\geq 1}$;
- $f(s,\,\cdot\,)\colon \mathbb{R}_{\geq 1} \to \mathbb{C}$ is piece-wise continuous for every $s \in D$;
- for every compact subset K of D there exists a piece-wise continuous function $g\colon \mathbb{R}_{\geq 1} \to \mathbb{R}$ such that

$$|f(s,\xi)| \leq g(\xi) \quad \text{for all} \quad (s,\xi) \in K \times \mathbb{R}_{\geq 1}\,, \qquad \text{and} \qquad \int_1^{\infty} g(\xi)\, d\xi < \infty\,.$$

Then the integral

$$F(s) = \int_1^\infty f(s,\xi)\,d\xi$$

converges (absolutely and uniformly) for all $s \in D$ and defines a holomorphic function $F\colon D \to \mathbb{C}$. Moreover,

$$F^{(k)}(s) = \int_1^\infty \frac{\partial^k}{\partial s^k} f(s,\xi)\,d\xi \quad \text{for all} \quad s \in D \quad \text{and} \quad k \in \mathbb{N}_0\,.$$

This result holds under much more general assumptions. However, this modest form using an elementary improper (Riemann) integral is sufficient for our purposes. For details we refer to [**3**])

B.2. Further analytic tools

We proceed with a series of probably less common analytic results. We start with the main applications of the Weierstrass criteria and prove basic facts on Dirichlet series and Dirichlet integrals. For a thorough introduction into the theory of Dirichlet series and their applications in number theory we refer to [**2**].

Lemma B.2.1 (Dirichlet integral)**.** *Let* $f\colon [1,\infty) \to \mathbb{C}$ *be piecewise continuous,* $B \in \mathbb{R}_{>0}$ *and* $\theta \in [0,1)$ *such that* $|f(x)| \le Bx^\theta$ *for all* $x \in [1,\infty)$*. Then the integral*

$$F(s) = \int_1^\infty \frac{f(\xi)}{\xi^{s+1}}\,d\xi$$

converges for all $s \in \mathcal{H}_\theta$ *and defines a holomorphic function* $F\colon \mathcal{H}_\theta \to \mathbb{C}$*. Moreover,*

$$F^{(k)}(s) = \int_1^\infty \frac{f(\xi)(-\log\xi)^k}{\xi^{s+1}}\,d\xi \quad \textit{for all} \quad s \in \mathcal{H}_\theta \quad \textit{and} \quad k \in \mathbb{N}_0\,.$$

Proof. If $K \subset \mathcal{H}_\theta$ is compact, then there exists some $\sigma \in \mathbb{R}_{>\theta}$ such that $K \subset \overline{\mathcal{H}}_\sigma$. However, if $\sigma \in \mathbb{R}_{>\vartheta}$, then

$$\Big|\frac{f(\xi)}{\xi^{s+1}}\Big| \le \frac{B}{\xi^{\sigma+1-\theta}} \quad \text{for all} \quad s \in \overline{\mathcal{H}}_\sigma \quad \text{and} \quad \int_1^\infty \frac{B}{\xi^{\sigma+1-\theta}}\,d\xi < \infty\,.$$

Hence the assertions follow by the Weierstrass criterion for integrals. □

Lemma B.2.2 (Dirichlet series)**.** *Let* $\mathsf{a}\colon \mathbb{N} \to \mathbb{C}$ *be a function and* $\vartheta \in \mathbb{R}_{>0}$ *such that*

$$\sum_{n=1}^\infty \frac{|\mathsf{a}(n)|}{n^\sigma} < \infty \quad \textit{for every } \sigma > \vartheta\,.$$

Then the Dirichlet series

$$F(s) = \sum_{n=1}^\infty \frac{\mathsf{a}(n)}{n^s} \quad \textit{and} \quad W(s) = \sum_{p\in\mathbb{P}} \sum_{j=1}^\infty \frac{\mathsf{a}(p^j)}{jp^{js}}$$

converge for all $s \in \mathcal{H}_\vartheta$ *and define holomorphic functions* $F, W\colon \mathcal{H}_\vartheta \to \mathbb{C}$. *Moreover,*

$$F^{(k)}(s) = \sum_{n=1}^{\infty} \frac{\mathsf{a}(n)(-\log n)^k}{n^s} \quad \textit{for all} \quad s \in \mathcal{H}_\vartheta \quad \textit{and} \quad k \in \mathbb{N}_0\,,$$

and if a *is bounded, then the assertions hold for* $\vartheta = 1$.

Proof. If $K \subset \mathcal{H}_\vartheta$ is compact, then there exists some $\sigma \in \mathbb{R}_{>\vartheta}$ such that $K \subset \overline{\mathcal{H}}_\sigma$, and since

$$\Big|\frac{\mathsf{a}(n)}{n^s}\Big| \le \frac{|\mathsf{a}(n)|}{n^\sigma} \quad \text{for all} \quad s \in \overline{\mathcal{H}}_\sigma\,.$$

we deduce from the Weierstrass criterion for series that $F\colon \mathcal{H}_\vartheta \to \mathbb{C}$ is holomorphic and the derivatives are as asserted.

To prove the assertion concerning W, we define $\mathsf{a}_1\colon \mathbb{N} \to \mathbb{C}$ by

$$\mathsf{a}_1(n) = \frac{\mathsf{a}(p^j)}{j} \quad \text{if} \quad n = p^j \quad \text{for some prime } p \text{ and } j \in \mathbb{N}, \quad \text{and } \mathsf{a}_1(n) = 0 \quad \text{otherwise.}$$

Then

$$W(s) = \sum_{n=1}^{\infty} \frac{\mathsf{a}_1(n)}{n^s}\,,$$

and since $|\mathsf{a}_1(n)| \le |\mathsf{a}(n)|$ for all $n \in \mathbb{N}$, the assertion follows.

Assume finally that a is bounded, and let $M \in \mathbb{R}_{>0}$ be such that $|\mathsf{a}(n)| \le M$ for all $n \in \mathbb{N}$. If $\sigma > 1$, then

$$\sum_{n=1}^{\infty}\Big|\frac{\mathsf{a}(n)}{n^\sigma}\Big| \le \sum_{n=1}^{\infty} \frac{M}{n^\sigma} < \infty$$

and therefore our assertions hold for $\vartheta = 1$. □

Exercise B.2.3. Under the assumptions of Lemma B.2.2 prove that the series defining $F(s)$ and its derivatives in fact converge uniformly in each closed half-plane $\overline{\mathcal{H}}_\sigma$ with $\sigma \in \mathbb{R}_{>\vartheta}$.

In the next lemma, we present partial summation, a standard technique of analytic number theory. With its help, we shall investigate the analytic behavior of functions given by Dirichlet series in the subsequent Theorem B.2.5 which is basic for the theory of L-functions in the Chapters 4 and 8.

Lemma B.2.4 (Partial summation). *Let* $\mathsf{a}\colon \mathbb{N} \to \mathbb{C}$ *be a function, and define*

$$\mathsf{A}\colon \mathbb{R}_{\ge 0} \to \mathbb{C} \quad \textit{by} \quad \mathsf{A}(\xi) = \sum_{n \le \xi} \mathsf{a}(n) \quad \textit{for all} \quad \xi \in \mathbb{R}_{\ge 0}$$

(*in particular,* $\mathsf{A}(\xi) = 0$ *if* $\xi < 1$). *Suppose that* $x, X \in \mathbb{R}$, $0 \le x < X$, *and let* $g\colon [x, X] \to \mathbb{C}$ *be continuously differentiable. Then*

$$\sum_{x < n \le X} \mathsf{a}(n) g(n) = \mathsf{A}(X) g(X) - \mathsf{A}(x) g(x) - \int_x^X \mathsf{A}(\xi) g'(\xi)\, d\xi\,.$$

If $g\colon [x,\infty) \to \mathbb{R}_{\geq 0}$ *is monotonically decreasing,* $M \in \mathbb{R}_{\geq 0}$ *and* $|\mathsf{A}(\xi)| \leq M$ *for all* $\xi \in \mathbb{R}_{\geq 0}$*, then*

$$\Bigg|\sum_{x<n\leq X} \mathsf{a}(n)g(n)\Bigg| \leq 3Mg(x)\,.$$

Proof. We set $c = \lfloor x \rfloor$ and $C = \lfloor X \rfloor$. Then A is constant on $[c,x]$, on $[C,X]$, and on each interval $[n,n+1)$ for $n \in \mathbb{N}_0$. Hence we obtain

$$\begin{aligned}\mathsf{A}(C)g(C)-\mathsf{A}(c)g(c) &= \mathsf{A}(X)g(C) - \mathsf{A}(x)g(c)\\ &= \mathsf{A}(X)g(X) - \mathsf{A}(x)g(x) - \mathsf{A}(X)\big[g(X)-g(C)\big] - \mathsf{A}(x)\big[g(c)-g(x)\big]\\ &= \mathsf{A}(X)g(X) - \mathsf{A}(x)g(x) - \int_C^X \mathsf{A}(\xi)g'(\xi)\,d\xi + \int_c^x \mathsf{A}(\xi)g'(\xi)\,d\xi\,,\end{aligned}$$

and

$$\begin{aligned}\sum_{x<n\leq X} \mathsf{a}(n)g(n) &= \sum_{n=c+1}^{C} \left[\mathsf{A}(n) - \mathsf{A}(n-1)\right]g(n) = \sum_{n=c+1}^{C} \mathsf{A}(n)g(n) - \sum_{n=c}^{C-1} \mathsf{A}(n)g(n+1)\\ &= \mathsf{A}(C)g(C) - \mathsf{A}(c)g(c) - \sum_{n=c}^{C-1} \mathsf{A}(n)\left[g(n+1)-g(n)\right]\\ &= \mathsf{A}(X)g(X) - \mathsf{A}(x)g(x) - \left\{\int_C^X + \int_x^c + \sum_{n=c}^{C-1}\int_n^{n+1}\right\}\mathsf{A}(\xi)g'(\xi)d\xi\\ &= \mathsf{A}(X)g(X) - \mathsf{A}(x)g(x) - \int_x^X \mathsf{A}(\xi)g'(\xi)\,d\xi\,.\end{aligned}$$

If $g\colon [x,\infty) \to \mathbb{R}_{\geq 0}$ is monotonically decreasing and $|\mathsf{A}(\xi)| \leq M$ for all $\xi \in \mathbb{R}_{\geq 0}$, then $|\mathsf{A}(X)g(X)| \leq Mg(x)$, $|\mathsf{A}(x)g(x)| \leq Mg(x)$,

$$\left|-\int_x^X \mathsf{A}(\xi)g'(\xi)d\xi\right| \leq \int_x^X |\mathsf{A}(\xi)|(-g'(\xi))d\xi \leq M\big(g(x)-g(X)\big) \leq Mg(x)\,,$$

and therefore

$$\Bigg|\sum_{x<n\leq X} \mathsf{a}(n)g(n)\Bigg| \leq 3Mg(x)\,. \qquad \square$$

Theorem B.2.5. *Let* $\mathsf{a}\colon \mathbb{N} \to \mathbb{C}$ *be a function such that*

$$\sum_{n=1}^{\infty} \frac{|\mathsf{a}(n)|}{n^\sigma} < \infty \quad \textit{for all} \quad \sigma > 1\,,$$

and define

$$\mathsf{A}\colon \mathbb{R}_{>0} \to \mathbb{C} \quad \textit{by} \quad \mathsf{A}(x) = \sum_{n\leq x} \mathsf{a}(n) \quad \textit{for all} \quad x \in \mathbb{R}_{>0}\,.$$

Let $F\colon \mathcal{H}_1 \to \mathbb{C}$ *be the holomorphic function defined by the Dirichlet series*

$$F(s) = \sum_{n=1}^{\infty} \frac{\mathsf{a}(n)}{n^s} \qquad (\textit{see } \text{Lemma B.2.2}).$$

Suppose that there exist real numbers $\lambda \in \mathbb{R}_{\geq 0}$, $\theta \in [0,1)$ *and* $B \in \mathbb{R}_{>0}$ *such that*

$$|\mathsf{A}(x) - \lambda x| \leq B x^{\theta} \quad \textit{for all} \quad x \in \mathbb{R}_{\geq 1}\,.$$

Then we have

$$F(s) = \frac{\lambda s}{s-1} + sG(s) \ \ \textit{for all } s \in \mathcal{H}_1, \quad \textit{where} \quad G(s) = \int_1^{\infty} \frac{\mathsf{A}(\xi) - \lambda\xi}{\xi^{s+1}}\, d\xi.$$

The function $G\colon \mathcal{H}_\theta \to \mathbb{C}$ *is holomorphic, and*

$$\lim_{s \to 1} (s-1)F(s) = \lambda\,.$$

In particular, F *extends to a holomorphic function* $F\colon \mathcal{H}_\theta \setminus \{1\} \to \mathbb{C}$, *and even to a holomorphic function* $F\colon \mathcal{H}_\theta \to \mathbb{C}$ *if* $\lambda = 0$.

Proof. We apply Lemma B.2.4 with $0 < x < 1 \leq X$ and $g(\xi) = \xi^{-s}$ for $s \in \mathcal{H}_1$. Since $g'(\xi) = -s\xi^{-s-1}$, we obtain

$$\begin{aligned}\sum_{n \leq X} \frac{\mathsf{a}(n)}{n^s} \ &= \sum_{x < n \leq X} \frac{\mathsf{a}(n)}{n^s} = \frac{\mathsf{A}(X)}{X^s} + s \int_1^X \frac{\mathsf{A}(\xi)}{\xi^{s+1}}\, d\xi \\ &= \frac{\mathsf{A}(X)}{X^s} + s \int_1^X \frac{\mathsf{A}(\xi) - \lambda\xi}{\xi^{s+1}}\, d\xi + \lambda s \int_1^X \frac{d\xi}{\xi^s}\,.\end{aligned}$$

If $s \in \mathcal{H}_\theta$, then Lemma B.2.1 implies that the integral

$$G(s) = \int_1^{\infty} \frac{\mathsf{A}(\xi) - \lambda\xi}{\xi^{s+1}}\, d\xi$$

converges and defines a holomorphic function $G\colon \mathcal{H}_\theta \to \mathbb{C}$. If $s \in \mathcal{H}_1$, then

$$\lim_{X \to \infty} \frac{\mathsf{A}(X)}{X^s} = 0 \quad \text{and} \quad \int_1^{\infty} \frac{d\xi}{\xi^s} = \frac{1}{s-1}\,.$$

Consequently, we obtain

$$F(s) = \frac{\lambda s}{s-1} + sG(s)\,, \quad \text{for all } s \in \mathcal{H}_1\,.$$

From this representation we see that F has an extension to a holomorphic function $F\colon \mathcal{H}_\theta \setminus \{1\} \to \mathbb{C}$, and even to a holomorphic function $F\colon \mathcal{H}_\theta \to \mathbb{C}$ if $\lambda = 0$. ☐

We close this section with a lemma on the connection between certain series and integrals. This is used in the proof of Theorem 4.3.5.

Lemma B.2.6. *Let* $f\colon \mathbb{R}_{\geq 1} \to \mathbb{R}_{\geq 0}$ *be piecewise continuous and decreasing. If* $x \in \mathbb{R}_{\geq 1}$, *then*

$$0 \ \leq \ \sum_{n \leq x} f(n) - \int_1^x f(\xi)\, d\xi \ \leq \ f(1)\,.$$

PROOF. Observe that

$$f(n+1) \leq \int_n^{n+1} f(\xi)\, d\xi \ \leq f(n) \quad \text{for all } \ n \in \mathbb{N}.$$

If $c = \lfloor x \rfloor$, then

$$\sum_{n \leq x} f(n) = \sum_{n=1}^{c} f(n) \ \geq \ \sum_{n=1}^{x} \int_n^{n+1} f(\xi)\, d\xi \ = \ \int_1^{c+1} f(\xi)\, d\xi \ \geq \ \int_1^{x} f(\xi)\, d\xi\,,$$

and

$$\sum_{n \leq x} f(n) - f(1) \ = \ \sum_{n=1}^{c-1} f(n+1) \ \leq \ \sum_{n=1}^{c-1} \int_n^{n+1} f(\xi)\, d\xi = \int_1^{c} f(\xi)\, d\xi \leq \int_1^{x} f(\xi)\, d\xi\,.$$

Hence it follows that

$$0 \ \leq \ \sum_{n \leq x} f(n) - \int_1^x f(\xi)\, d\xi \ \leq \ f(1)\,. \qquad \square$$

This page intentionally left blank

Bibliography

[1] A. Aigner, *Zahlentheorie*, de Gruyter, 1975.

[2] T. M. Apostol, *Introduction to Analyic Number Theory*, Springer, 1976.

[3] T.M. Apostol, *Mathematical analysis*, Addison-Wesley, 1971.

[4] T. Azuhata, *On the fundamental units and class numbers of real quadratic fields*, Nagoya Math. J. **95** (1984), 125 – 135.

[5] P. Bateman, A. Hildebrand, and G.B. Purdy, *Sums of distinct squares*, Acta Arith. **67** (1994), 349 –380.

[6] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi Sums*, J. Wiley, 1998.

[7] M. Bhargava, *On the Conway-Schneeberger Fifteen Theorem*, Quadratic forms and their applications (Dublin, 1999), Contemp. Math., vol. 272, Amer. Math. Soc., Providence, RI, 2000, pp. 27 – 37.

[8] ______, *Higher composition laws and applications*, International Congress of Mathematicians. Vol. II (Zürich), Eur. Math. Soc., 2006, pp. 271 – 294.

[9] J. Brillhart, *Note on Representing a Prime as a Sum of Two Squares*, Math. Comp. **26** (1972), 1011 – 1013.

[10] D. Brink, *Five peculiar theorems on simultaneous representation of primes by quadratic forms*, J. Number Theory **129** (2009), 464–468.

[11] E. Brown, *A theorem on biquadratic reciprocity*, Proc. Amer. Math. Soc. **30** (1971), 220 – 222.

[12] J. Brüdern, *Einführung in die analytische Zahlentheorie*, Springer, 1995.

[13] D. A. Buell, *Binary Quadratic Forms, Classical Theory and Modern Computations*, Springer, 1989.

[14] P. Bundschuh, *Einführung in die Zahlentheorie*, Springer, 1996.

[15] K. Burde, *Ein rationales biquadratisches Reziprozitätsgesetz*, J. Reine Angew. Math. **235** (1969), 175 – 184.

[16] H. Cohen, *A course in computational algebraic number theory*, Springer, 1993.

[17] ______, *Number Theory. Volume I: Tools and Diophantine Equations*, Springer, 2007.

[18] H. Cohn, *A Classical Invitation to Algebraic Numbers and Class Fields*, Springer, 1978.

[19] D. A. Cox, *Primes of the form* $x^2 + ny^2$, J. Wiley, 1989.

[20] H. Davenport, *Multiplicative Number Theory*, Springer, 1980.

[21] L. E. Dickson, *Modern Elementary Theory of Numbers*, Univ. of Chicago Press, 1939.

[22] ______, *History of the Theory of Numbers*, Chelsea Reprint, 1971.

[23] P. G. L. Dirichlet, *Vorlesungen über Zahlentheorie*, Chelsea Reprint 1968, 1893.

[24] H. M. Edwards, *Divisor Theory*, Birkhäuser, 1990.

[25] L. L. Littlejohn F. W. Clarke, W. N. Everitt and S. J. R. Vorster, *H. J. S. Smith and the Fermat Two Squares Theorem*, Amer. Math. Monthly **106** (1999), 652 – 665.

[26] W. Feit, *Some Diophantine equations of the form* $x^2 - py^2 = z$, Proc. Amer. Math. Soc. **129** (2000), 623 – 625.

[27] D. Flath, *Introduction to Number Theory*, J. Wiley, 1989.

[28] G. Frei, *Leonard Euler's convenient numbers*, Math. Intelligencer **3** (1985), 55 – 58, 64.

[29] C. Friesen, *Legendre symbols and coninued fractions*, Acta Arith. **59** (1991), 365 – 379.

[30] A. Fröhlich, *The restricted biquadratic residue symbol*, Proc. London Math. Soc. **9** (1959), 189 – 207.

[31] Y. Furuta, *Norms of units of quadratic fields*, J. Math. Soc. Japan **11** (1958), 139 – 145.

[32] C. F. Gauss, *Disquisitiones Arithmeticae*, Springer, 1966.

[33] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics, vol. 278, Chapman & Hall/CRC, 2006.

[34] E. Grosswald, *Representations of Integers as Sums of Squares*, Springer, 1985.

[35] F. Halter-Koch, *Darstellung natürlicher Zahlen als Summe von Quadraten*, Acta Arith. **42** (1982), 11 – 20.

[36] ______, *Über Pell'sche Gleichungen und Kettenbrüche*, Arch. Math. **49** (1987), 29 – 37.

[37] ______, *Einige periodische Kettenbrüche und Grundeinheiten quadratischer Ordnungen*, Abh. Math. Semin. Univ. Hamb. **59** (1989), 157 – 169.

[38] ______, *Reell-quadratische Zahlkörper mit großer Grundeinheit*, Abh. Math. Semin. Univ. Hamb. **59** (1989), 171 – 181.

[39] ______, *Diophantine equations of Pellian type*, J. Number Theory **131** (2011), 1597 – 1615.

[40] F. Halter-Koch, P. Kaplan, K. S. Williams, and Y. Yamamoto, *Infrastructure des classes ambiges d'ideaux des ordres des corps quadratiques réels*, L'Ens. Math. **37** (1991), 263 – 292.

[41] K. Hardy and K. S. Williams, *Congruences modulo* 16 *for the Class Numbers of Complex Quadratic Fields*, J. Number Theory **27** (1987), 178 – 195.

[42] H. Hasse, *Vorlesungen über Zahlentheorie*, Springer, 1950.

[43] L. K. Hua, *Introduction to Number Theory*, Springer, 1982.

[44] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, 1990.

[45] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, AMS Colloquium Publ., 2004.

[46] Ch. U. Jensen, *On the solvability of a certain class of non-pellian equations*, Math. Scand. **10** (1962), 71 – 84.

[47] M. J. Jacobson Jr. and H. C. Williams, *The size of the fundamental solutions of consecutive Pell equations*, Experiment. Math. **9** (2000), 631 – 640.

[48] B. Jun and J. Lee, *Caliber of quadratic fields*, J. Number Theory **130** (2010), 2586 – 2595.

[49] B. Goddard K. Cheng and R. A. Mollin, *The Diophantine equation $ax^2 - by^2 = c$ solved via continued fractions*, Acta Math. Univ Commenianae **71** (2002), 1 – 18.

[50] K. Hardy K. S. Williams and C. Friesen, *On the evaluation of the Legendre symbol* $\left(\frac{A+B\sqrt{m}}{p}\right)$, Acta Arith. **45** (1985), 255 – 272.

[51] P. Kaplan, *Cours d'arithmétique*, U.E.R. des Sci. Math. Univ. Nancy I, 1972.

[52] ______, *Divisibilité par* 8 *du nomble des classes des corps quadratiques dont le* 2*-groupe des classes est cyclique, et réciprocité biquadratique*, J. Math. Soc. Japan **25** (1973), 596 – 608.

[53] ______, *Sur le* 2*-groupe des classes d'idéaux des corps quadratiques*, J. Reine Angew. Math. **283/284** (1976), 313 – 363.

[54] ______, *Cycles d'ordre au moins* 16 *dans le deux groupe des classes d'idéaux au sense strict de corps quadratiques*, Bull. Soc. Máth. France Mém. **49/50** (1977), 113 – 124.

[55] ______, *On the class numbers of* $\mathbb{Q}(\sqrt{\pm 2p})$ *modulo* 16*, for* $p \equiv 1 \pmod 8$*, a prime*, Acta Arith. **40** (1982), 289 – 296.

[56] ______, *A propos des équations antipelliennes*, Enseign. Math. **29** (1983), 323 – 328.

[57] P. Kaplan and K. S. Williams, *Congruences modulo* 16 *for the class numbers of the quadratic fields* $\mathbb{Q}(\sqrt{\pm p})$ *and* $\mathbb{Q}(\sqrt{\pm 2p})$ *for* p *a prime congruent to* 5 *modulo* 8, Acta Arith. **15** (1982), 375 – 397.

[58] ______, *The distance between ideals in the orders of a real quadratic field*, Enseign. Math. **36** (1990), no. 3, 321–358.

[59] P. Kaplan, K. S. Williams, and K. Hardy, *Divisibilité par* 16 *du nombre des classes au sense strict des corps quadratiques réels dont le deux groupe des classes est cyclique*, Osaka J. Math **23** (1986), 479 – 489.

[60] I. Kaplansky, *The forms $x^2 + 32y^2$ and $x^2 + 64y^2$*, Proc. Amer. Math. Soc. **131** (2003), no. 7, 2299–2300.

[61] O.-H. Keller, *Über die Numeri idonei von Euler*, Beiträge Algebra Geom. **16** (1983), 79 – 91.

[62] H. Koch, *Zahlentheorie*, Vieweg, 1997.

[63] G. Lachaud, *On real quadratic fields*, Bull. Amer. Math. Soc. **17** (1987), 307 – 311.

[64] S. Lang, *Algebra, 3rd rev. ed.*, Springer, 2002.

[65] M. D. Larsen and P. J. McCarthy, *Multiplicative Theory of Ideals*, Academic Press, 1971.

[66] E. Lehmer, *Criteria for cubic and quartic residuacity*, Mathematik **5** (1958), 20 – 29.

[67] F. Lemmermeyer, *Reciprocity Laws*, Springer, 2000.

[68] P. A. Leonard and K. S. Williams, *On the divisibility of the class numbers of* $\mathbb{Q}(\sqrt{-p})$ *and* $\mathbb{Q}(\sqrt{-2p})$ *by* 16, Canadian Math. Bull. **25** (1982), 200 – 206.

[69] ——, *On the divisibility of the class number of* $\mathbb{Q}(\sqrt{-pq})$ *by* 16, Proc. Edinburgh Math. Soc. **26** (1983), 221 – 231.

[70] H. Lüneburg, *Vorlesungen über Zahlentheorie*, Birkhäuser, 1978.

[71] R.J. McIntosh and E.L. Roettger, *A search for Fibonacci-Wieferich and Wolstenholme primes*, Math. Comp. **76** (2007), 2087 – 2094.

[72] F. Mertens, *Ein Beweis des Satzes, daß jede Klasse von ganzzahligen primitiven binären quadratischen Formen des Hauptgeschlechts durch Duplikation entsteht*, J. Reine Angew. Math. **129** (1905), 181 – 186.

[73] R. A. Mollin, *The Palidromic Index - A Measure of Ambiguous Cycles of Reduced Ideals Without any Ambiguous Ideals in Real Quadratic Orders*, J. Th. Nomb. Bordeaux **7** (1995), 447 – 460.

[74] ——, *Quadratics*, CRC Press, 1996.

[75] ——, *Solutions of Diophantine equations and divisibility of class numbers of complex quadratic fields*, Glasgow Math. J. **38** (1996), 195 – 197.

[76] ——, *Jacobi symbols, ambiguous ideals, and continued fractions*, Acta Arith. **85** (1998), 331 – 349.

[77] ——, *A continued fraction approach to the Diophantine equation* $ax^2 - by^2 = \pm 1$, JP Journal of Algebra, Number Theory and Appl. **4** (2004), 565 – 571.

[78] R. A. Mollin and K. Cheng, *Beepers, creepers and sleepers*, Int. Math. J. **2** (2002).

[79] R. A. Mollin and A. J. van der Poorten, *Continued fractions, Jacobi Symbols, and Quadratic Diophantine Equations*, Canadian Math. Bull. **43** (2000), 218 – 225.

[80] R. A. Mollin and H. C. Williams, *A complete generalization of Yokoi's p-invariants*, Colloq. Math. **63** (1992), 285 – 294.

[81] P. Morton, *On Rédei's theory of the Pell equation*, J. Reine Angew. Math. **307/8** (1979), 373 – 398.

[82] W. Narkiewicz, *Global class-field theory*, Handbook of Algebra I (1996), 365 – 393.

[83] ——, *Elementary and Analytic Theory of Algebraic Numbers*, Springer, 2004.

[84] ——, *Rational Number Theory in the 20th Century*, Springer, 2011.

[85] J. Neukirch, *Algebraic Number Theory*, Springer, 1999.

[86] J. Oesterle, *Le probléme de Gauss sur le nombre de classes*, L'Ens. Math. **34** (1988), 43 – 67.

[87] G. Pall, *On sums of squares*, Amer. Math. Monthly **40** (1933), 10 – 18.

[88] ——, *Discriminantal Divisors of Binary Quadratic Forms*, J. Number Theory **1** (1969), 525 – 533.

[89] R. D. Patterson, A. J. van der Poorten, and H. C. Williams, *Characterization of a generalized Shanks sequence*, Pacific J. Math. **230** (2007), 951 – 956.

[90] O. Perron, *Die Lehre von den Kettenbrüchen*, B. G. Teubner, 1989.

[91] P.T.A.Elliott, *Probabilistic Number Theory I*, Springer, 1979.

[92] P. Ribenboim, *My Numbers, My Friends*, Springer, 2000.

[93] A. Scholz, *Über die Lösbarkeit der Gleichung* $t^2 - du^2 = -4$, Math. Z. **39** (1934), 95 – 111.

[94] T. Schönemann, *Theorie der symmetrischen Funktionen der Wurzeln einer Gleichung. Allgemeine Sätze über Congurenzen nebst einigen Anwendungen derselben*, J. Reine Angew. Math. **19** (1839), 289 – 308.

[95] N. Sedrakian and J. Steinig, *A particular case of Dirichet's theorem on arithmetic progressions*, L'Ens. Math. **44** (1998), 3 – 7.

[96] A. Selberg, *An elementary proof of Dirichlet's theorem about primes in an arithmetic progression*, Ann. of Math. **50** (1940), 305 – 313.

[97] J. A. Serret, *Note sur un théorème de la théorie des nombres*, J. Math. Pures Appl. **17** (1852), 186 – 189.

[98] D. Shanks, *On Gauss's class-number problem*, Math. Comp. **23** (1969), 151 – 163.

[99] W. Sierpiński, *Elementary Theory of Numbers*, North-Holland, 1988.

[100] H. Stark, *On complex quadratic fields with class-number* 2, Math. Comp. **29** (1975), no. 1, 289 – 302.

[101] Z.-H. Sun, *Supplements to the theory of quartic residues*, Acta Arith. **97** (2001), no. 4, 361–377.

[102] ———, *Quartic residues and binary quadratic forms*, J. Number Theory **113** (2005), 10–52.

[103] A. J. van der Poorten and P. G. Walsh, *A Note on Jacobi Symbols and Continued Fractions*, Amer. Math. Monthly **106** (1999), 52 – 56.

[104] B. A. Venkov, *Elementary number theory*, Woolters-Noordhoff, 1970.

[105] D.D. Wall, *Fibonacci sequence modulo* m, Amer. Math. Monthly **67** (1960), 525 – 532.

[106] W. C. Waterhouse, *The sign of the Gaussian sum*, J. Number Theory **2** (1970), 363.

[107] A. Weil, *Number Theory. An approach through history. From Hammurapi to Legendre*, Birkhäuser, 1983.

[108] P. Weinberger, *Real quadratic fields with class number divisible by* n, J. Number Theory **5** (1973), 237 – 241.

[109] E.T. Whittaker and G.N. Watson, *A course of modern analysis*, Cambridge Univ. Press, 1935.

[110] K. S. Williams, *On the class number of* $\mathbb{Q}(\sqrt{-p})$ *modulo* 16, *for* $p \equiv 1 \bmod 8$ *a prime*, Acta Arith. **39** (1981), 381 – 398.

[111] K. S. Williams and N. Buck, *Comparison of the lengths of the continued fractions of* $\sqrt{D}$ *and* $\frac{1}{2}(1+\sqrt{D})$, Proc. Amer. Math. Soc. **120** (1994), no. 4, 995 – 1002.

[112] Y. Yamamoto, *On unramified Galois extensions of quadratic number fields*, Osaka J. Math. **7** (1970), 57 – 76.

[113] ———, *Real quadratic fields with large fundamental units*, Osaka J. Math. **8** (1971), 261 – 270.

[114] ———, *Divisibility by* 16 *of class number of quadratic fields whose* 2*-class groups are cyclic*, Osaka J. Math. **21** (1984), 1 – 22.

[115] H. Yokoi, *On real quadratic fields containing units with norm* -1, Nagoya Math. J **33** (1968), 139 – 152.

[116] ———, *On the fundamental unit of real quadratic fields with norm* 1, J. Number Theory **2** (1970), 106 – 115.

[117] D. B. Zagier, *Zetafunktionen und quadratische Körper*, Springer, 1981.

List of Symbols

$(a_1,\dots,a_n)=1$, 366, 391
$A^\bullet$, xiii
$D_{[b]}$, 393
$F_1 * F_2$, 214
$G_p,\ G[p],\ r_p(G)$, 379
$I(\xi)$, 136
K^+, 142
$L(s,\chi),\ \Lambda(s,\chi),\ \zeta(s)$, 107
$L_\Delta(s,\phi),\ \Lambda_\Delta(s,\phi),\ \zeta_\Delta(s)$, 333
$R^\bullet,\ R^\times,\ \mathsf{q}(R)$, 362
$[\mathfrak{a}]^{(+)},\ \mathcal{S}_K^{(+)}$, 140
$[a_1,\dots,a_n],\ \langle a_1,\dots,a_n\rangle$, xiii, 362
$[u_1,\dots,u_n]$, 25
$[u_0,u_1,\dots]$, 29
$\Delta^*,\ c(\Delta)$, 84
Δ_K, 6
$\Delta_f,\ d_f,\ M_f,\ \xi_f$, 191
$\mathrm{Ker}(\varphi),\ \mathrm{Im}(\varphi)$, 360
$\mathbb{R}_{>0},\ \mathbb{R}_{\ge 0},\ \mathbb{Q}_{>0},\ \mathbb{N}_{\ge 2}$, etc., $[a,b]$, sgn, xiii
$\Re(z),\ \Im(z),\ \sqrt{z},\ \lfloor x\rfloor,\ \lceil x\rceil$, xiii
$\mathbb{Z}[z_1,\dots,z_n],\ \mathbb{Z}[z]$, 395
$\left(\frac{N}{n}\right)$, 76
$\left(\frac{\alpha}{\beta}\right)_3$, 260, 262
$\left(\frac{\alpha}{\beta}\right)_2$, 274, 275
$\left(\frac{\alpha}{\beta}\right)_4$, 273, 275
$\left(\frac{a}{p}\right)$, 72
$\left(\frac{n}{m}\right)$, 76, 82
$\left[\frac{a}{m}\right]_4$, 289
χ_π, 273
$\lambda_\Delta,\ \mathsf{w}_\Delta$, 325
$\mathrm{lcm}(a_1,\dots,a_n)$, 367
$\gcd(a_1,\dots,a_n)$, 366
$\mathbb{W},\ \mathbb{W}_n,\ \mathbb{W}^*,\ \mathbb{W}(D)$, 384
$\mathscr{F}_\Delta,\ \mathscr{F}_\Delta^\times,\ \mathscr{I}_\Delta,\ \mathfrak{N}_\Delta(\mathfrak{a})$, 132
$\mathscr{I}_\Delta^*$, 322
$\mathscr{I}_\Delta^{(\alpha)}$, 182
$\mathsf{J}(\chi_1,\chi_2)$, 70
$\mathsf{M}_{m,n},\ \mathsf{M}_n,\ \mathsf{GL}_n,\ \mathsf{SL}_n$, 364
Q_Δ, 85
$\mathsf{X}(m),\ \mathbf{1}_m$, 67
$\mathsf{e},\ \mathsf{i}$, xiii
$\mathsf{p}(\xi)$, 53
v_p, 368
$\mathrm{Aut}(f)$, 198
$\mathcal{A}_\Delta^{(+)},\ \mathcal{A}_\Delta^*,\ \mu(\Delta)$, 157
$\mathcal{C}_K$, 177
$\mathcal{F}$, 12
$\mathcal{H}_\theta,\ \overline{\mathcal{H}}_\theta$, xiii, 399
$\mathcal{L}(K),\ (\mathfrak{a} :_K \mathfrak{b})$, 116
$\mathcal{N}(\xi),\ \mathcal{T}(\xi),\ \xi'$, 1
$\mathcal{O}_\Delta,\ \mathcal{O}_K$, 118
$\mathcal{O}_\Delta^\times$, 122
$\mathcal{O}_\Delta^{\times +}$, 124
$\mathcal{R}(\mathfrak{a})$, 117
$\mathcal{S}_\Delta^{(+)},\ \mathcal{C}_\Delta^{(+)}$, 141
$\mathfrak{A}_\Delta$, 340
$\mathfrak{C}_\Delta,\ \mathscr{P}_\Delta$, 332
$\mathfrak{F}_\Delta,\ \llbracket f\rrbracket,\ \llbracket a,b,c\rrbracket$, 197
$\mathfrak{H}^+,\ \mathfrak{H}^-$, 7
$\mathfrak{X}_\Delta,\ \mathfrak{X}_\Delta^+$, 19
$h_\Delta,\ h_\Delta^+$, 20
$\omega_\Delta,\ \sigma_\Delta$, 4
ord, 375
$\overline{\mathbb{Q}},\ \overline{\mathbb{Z}}$, 395
$\sim,\ \sim_+$, 12, 140
$\tau(\chi,a),\ \tau(\chi)$, 68
θ_π, 260
ε_Δ, 44
$\varphi(m)$, 381
$\widehat{G},\ \widehat{G}[2],\ \mathbf{1}$, 386
$\xi^\#$, 17
$a \mid b,\ (a_1,\dots,a_n)$, 366
$f^-,\ f^{\mathsf{op}},\ g_\Delta$, 193
f_Δ, 5
$h_\Delta,\ h_\Delta^+,\ h_K,\ h_K^+$, 146
$l(\xi)$, 41
$\mathrm{Stab}(\xi),\ \mathrm{Stab}^+(\xi),\ \mathfrak{M}$, 8

This page intentionally left blank

Algebra

Quadratic Irrationals

An Introduction to Classical Number Theory

Quadratic Irrationals: An Introduction to Classical Number Theory gives a unified treatment of the classical theory of quadratic irrationals. Presenting the material in a modern and elementary algebraic setting, the author focuses on equivalence, continued fractions, quadratic characters, quadratic orders, binary quadratic forms, and class groups.

The book highlights the connection between Gauss's theory of binary forms and the arithmetic of quadratic orders. It collects essential results of the theory that have previously been difficult to access and scattered in the literature, including binary quadratic Diophantine equations and explicit continued fractions, biquadratic class group characters, the divisibility of class numbers by 16, F. Mertens' proof of Gauss's duplication theorem, and a theory of binary quadratic forms that departs from the restriction to fundamental discriminants. The book also proves Dirichlet's theorem on primes in arithmetic progressions, covers Dirichlet's class number formula, and shows that every primitive binary quadratic form represents infinitely many primes. The necessary fundamentals on algebra and elementary number theory are given in an appendix.

Research on number theory has produced a wealth of interesting and beautiful results yet topics are strewn throughout the literature, the notation is far from being standardized, and a unifying approach to the different aspects is lacking. Covering both classical and recent results, this book unifies the theory of continued fractions, quadratic orders, binary quadratic forms, and class groups based on the concept of a quadratic irrational.

K20533

ISBN: 978-1-4665-9183-7
90000
9 781466 591837

CRC Press
Taylor & Francis Group
an **informa** business
www.crcpress.com

6000 Broken Sound Parkway, NW
Suite 300, Boca Raton, FL 33487
711 Third Avenue
New York, NY 10017
2 Park Square, Milton Park
Abingdon, Oxon OX14 4RN, UK